AIA House,
74 Taharoto Road,
Takapuna,
Auckland 0622
-
Private Bag 92499,
Victoria Street West,
Auckland 1142

Phone (Int.) +64 9 487 9963
Freephone 0800 500 108
-
enquireNZ@aia.com
aia.co.nz

24 July 2023

Consumer Policy Team
Building Resources and Markets
Ministry of Business, Innovation and Employment
PO Box 1473
Wellington 6140

By email: consumerdataright@mbie.govt.nz

CUSTOMER AND PRODUCT DATA BILL EXPOSURE DRAFT AND CONSULTATION PAPER

This submission is made on behalf of AIA New Zealand Limited and its related entities (together **AIA NZ**). It is in response to the Ministry of Business, Innovation and Employment's (**MBIE**) June 2023 discussion document "Unlocking value from our customer data" (**Discussion Document**) and the related exposure draft Customer and Product Data Bill (the **Bill**).

About AIA NZ

AIA NZ is a member of the AIA Group, which comprises the largest independent publicly listed pan-Asian life insurance group. It has a presence in 18 markets in Asia-Pacific and is listed on the Main Board of The Stock Exchange of Hong Kong. It is a market leader in the Asia-Pacific region (excluding Japan) based on life insurance premiums and holds leading positions across the majority of its markets.

Established in New Zealand in 1981, AIA NZ is New Zealand's largest life insurer and has been in business in New Zealand for over 40 years. AIA NZ's vision is to champion New Zealand to be the healthiest and best protected nation in the world.

AIA NZ offers a range of life and health insurance products that meet the needs of over 815,000 New Zealanders. AIA NZ is committed to an operating philosophy of Doing the Right Thing, in the Right Way, with the Right People.

AIA NZ is also a prominent member of the Financial Services Council (**FSC**).

Key submission points

AIA NZ supports the objectives of giving customers greater control over their data to unlock value and innovation which can utilise this data. AIA NZ supports the protection of customers' data and personal information and takes the protection of our customer information seriously.

Our submission in response to the Discussion Document is **attached** in which we only respond to questions posed by MBIE where we can provide a view. Our key points are summarised below:

- The Bill is unclear in a number of respects as to how it will operate in practice. It is difficult to assess as the detail is left to standards and secondary legislation which will be developed at a later date. We appreciate a balance needs to be struck to allow for a flexible regime supporting a sectorial designation approach, however some of the core issues that the Discussion Document and Bill contemplate being addressed in secondary legislation are fundamental to the regime and the protection of customer data and should be addressed in the Bill.

- We believe that the Bill does not provide for adequate protections of customer data. While the Bill relies on the Privacy Act 2020 (**Privacy Act**) in many respects, the specific nature of the Bill creates uncertainty and has the potential to create dual regulatory regimes for participants. We think that specific protections and safeguards should be included in the Bill to protect customers data as this is fundamental to customer and business trust in the system.

- We disagree with MBIE's view that accredited requestors or intermediaries should be able to share customer information obtained under the Bill with third parties provided the Privacy Act is complied with. In our view all recipients of customer data should be accredited requestors including intermediaries. An accredited requestor should not be permitted to share data obtained from a data holder with a third party unless the customer has expressly consented, and the third party is also accredited. We think that this requirement is fundamental to customer trust and confidence in the regime and ensuring that the high standards of storage, security and ethics are maintained by data holders and all those who receive customer data.

We would be pleased to discuss any questions you have on this submission, and we would welcome the opportunity to collaborate or consult further with MBIE as it considers the next steps.

Yours sincerely

Privacy of natural persons

General Counsel and Company Secretary
AIA New Zealand Limited

Submission on discussion document: *Unlocking value from our customer data*

Your name and organisation

Name	Privacy of natural persons
Organisation (if applicable)	AIA New Zealand Limited
Contact details	Privacy of natural persons

[Double click on check boxes, then select 'checked' if you wish to select any of the following.]

☒ The Privacy Act 2020 applies to submissions. Please check the box if you do not wish your name or other personal information to be included in any information about submissions that MBIE may publish.

☐ MBIE intends to upload submissions received to MBIE's website at ***www.mbie.govt.nz***. If you do not want your submission to be placed on our website, please check the box and type an explanation below.

I do not want my submission placed on MBIE's website because… [Insert text]

Please check if your submission contains confidential information:

☒ I would like my submission (or identified parts of my submission) to be kept confidential, and **have stated below** my reasons and grounds under the Official Information Act that I believe apply, for consideration by MBIE.

I would like identified parts of our submission to be kept confidential as these sections contain information that is commercially sensitive in nature, and disclosure of this information could prejudice our commercial position.

Responses to discussion document questions

How will the draft law interact with protections under the Privacy Act?

1	*Does the proposed approach for the interaction between the draft law and the Privacy Act achieve our objective of relying on Privacy Act protections where possible? Have we disapplied the right parts of the Privacy Act?*

AIA NZ agrees that the Bill should rely on the existing privacy protections under the Privacy Act where possible. However, in our view, there is still significant ambiguity as to how the overlap between the Privacy Act and the Bill will work at an operational level, and the current approach has the potential to create dual regulatory regimes for participants. It is also difficult to comment on the risks of this approach when there is a broad discretion to impose more detailed requirements in secondary legislation, which is yet to be developed, particularly as there has been very limited engagement with industries outside of the banking sector.

We appreciate the intention that, rather than replace the protections in the Privacy Act or impose a new regime that sits alongside the Privacy Act, the Bill will rely on existing protections in the Privacy Act and "top-up" privacy protections as needed. However, it is not clear that relying on existing protections will simplify compliance, as data holders will likely hold a mix of designated data and non-designated data, in each case with a mix of personal and non-personal information. As a result, data holders will be subject to two overlapping regimes.

The two regimes are difficult to reconcile as the Privacy Act takes a flexible, principles-based approach to the protection of personal information, in order to apply across the economy, whereas the customer data right (**CDR**) regime will apply detailed rules and technical standards to designated sectors. Where MBIE considers that the specific requirements under the Bill are consistent with existing protections in the Privacy Act, that does not mean that the Office of the Privacy Commissioner (**OPC**) (or the Human Rights Review Tribunal) will take the same view.

In addition, the proposed approach to address the overlap between Information Privacy Principle (**IPP**) 6 requests and requests under the Bill is ambiguous. It is unclear from the drafting of clause 44 whether a request for customer data that includes both personal and non-personal information will be treated: (a) entirely as an IPP 6 request; or (b) as an IPP 6 request in relation to the personal information within the request, and as a customer data request under the Bill in relation to all other customer data.

Our assumption is that clause 44 is not intended to extend the scope of IPP 6 requests to cover non-personal information however, we think this needs to be clarified in the drafting of the Bill. Even if this assumption is correct, it is unclear what this would mean in practice – in particular, if a request covered personal and non-personal information:

- Would the data holder be responsible for identifying whether specific data in a request is personal information, and therefore subject to the safeguards in sections 49 to 53 of the Privacy Act, or non-personal information?
- If some of the data in a request is withheld under one of the grounds in sections 49 to 53, should the rest of the data still be provided even if it is unlikely to be useful without the personal information?
- If a data holder does not comply with a request, who would be responsible for investigating this issue, and for enforcing a breach?

Although the Discussion Document notes an intention to address the overlap of responsibilities between the OPC and MBIE in an MOU, it is unlikely that an MOU is the appropriate legal tool to address these issues – this should be addressed in the Bill.

Consent settings: respecting and protecting customers' authority over their data

General comments on consent

AIA NZ agrees that data holders are best placed to confirm that consents are valid and that information requested aligns with the consent provided, and that this is an important check to protect customers against unauthorised use or disclosure of their data. In general, however, it is difficult to provide feedback on the proposed approach to consent as the Bill provides limited detail on what will be required in practice and there is a broad discretion to prescribe, in regulations or standards, specific requirements about the manner in which authorisation is given or confirmed. Without these details, AIA NZ cannot assess the level of work and resources that its obligations under the Bill will likely require.

In particular, AIA NZ is concerned about the Bill's requirement for data holders to confirm that a requested service is within the scope of the authorisation provided by a customer before providing regulated data. Confirmation must be carried out in the manner prescribed by the regulations and the standards (if any). Without further details being prescribed in the regulations or standards, this requirement would seemingly require a close review of the consent given, the request made, and the data to be provided, which will take significant dedicated time and resources. In our view the Bill should prescribe a default method for authorisation and confirmation which applies unless a more specific method is set in regulations.

AIA NZ notes that clause 14 of the Bill provides for customers to access their data using the same system used by data requestors to transmit data to an accredited requestor. Customers are already given access to their data in a number of ways by data holders including using apps, online platforms and upon request. We are concerned that by enabling customers to access their data in the same format as accredited requestors, there is a risk that alternative platforms that are not accredited could use the same screen scraping technology that is currently in place to scrape data from banking systems. We believe this could lead to data breaches, security vulnerabilities and / or malicious use of a customer's data as it is exposed in a machine-readable format. We agree that customers should be able to access their data but that this should not be at the expense of cyber security and privacy protections. In our view, the data sharing system established under the CDR regime should only be used to transmit data from a data holder to an accredited requestor to ensure the highest cyber security safeguards are applied and followed.

2 *Should there be a maximum duration for customer consent? What conditions should apply?*

AIA NZ agrees that a maximum duration for customer consent should be set in the Bill and that any inconvenience this may create is outweighed by the protection of personal information and customer data. We suggest that a six-month consent period with a short form re-confirmation might be appropriate to balance the inconvenience of frequent reconfirmations and the increased risk of unintentionally losing access to data-enabled services, against the need for strong data protection and customer understanding of who has access to their data to ensure that customer consent is ongoing and informed. We also suggest that the Bill is the appropriate place for this maximum duration to be set as it reinforces the importance of informed customer consent.

If there is a maximum duration for customer consent, the Government should clarify that where a customer reconfirms their authorisation, without modification, prior to the expiry of the then-current authorisation, the data holder is not required to recheck that any existing regulated data services being provided are within the scope of the authorisation given under clause 33(5) of the Bill.

4 *Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*

AIA NZ agrees with the proposed circumstances in which consent should automatically end.

We suggest the addition of the following circumstances:

- when an accredited requestor ceases to be accredited; and
- when a data holder becomes aware that the customer has died.

The Government should carefully consider the impact of a customer's death on the application of the Bill. Particularly because if authorisation does not end when a customer dies, the protection given to the customer's data is significantly reduced as the Privacy Act only applies to information about living persons.

We also recommend that, in addition to the circumstances identified under clause 72 of the Bill, the chief executive of MBIE (**Chief Executive**) should have the right to cancel or suspend a requestor's accreditation (which would then end any related authorisations) in the event of a significant data breach or where an accredited requestor is found to be in breach of the accreditation requirements (e.g. security standards).

We disagree with the proposal that regulations should specify that consent ceases upon a customer closing their account with a data holder as there may be valid reasons why customers may want to continue to provide accredited requestors with access to their data, such as where a data-enabled service relates to lending applications where historical transaction data may be relevant.

6 *What are your views on the proposed obligations on data holders and accredited requestors in relation to consent, control, and accountability? Should any of them be changed? Is there anything missing?*

AIA NZ agrees that the proposed obligations appropriately hold data holders and accredited requestors accountable.

We think that the requirement for ending consent to be as easy as providing consent will be difficult to achieve in practice because consent will often be provided as part of signing up for a service (for example, when a customer is signing up to an accredited requestor's service it is likely that the customer will be prompted to provide their authorisation during the onboarding process), while withdrawing consent may need to be done in a settings or preference menu. We consider that clarifying the scope of this requirement would assist and that alignment with the requirements under the Unsolicited Electronic Messages Act 2007 may be appropriate.

We note the requirements to communicate with customers when consent is given and ends, and when a request is actioned. We have concerns that customers could experience notification fatigue as it is unclear what timeframes apply to these notifications and if a customer changes their consent multiple times in a short amount of time, they could receive multiple notifications. We consider that data holders should be able to aggregate communications to customers to reduce the number of communications a customer receives.

In addition, we think that the Bill should clarify that consent from a customer can only be provided to a data holder electronically using the system operated by the data holder for that purpose. This would streamline the consent process and ensure that customers receive appropriate information about the consent they are providing. We believe it is necessary to ensure that the data holder does not receive customer consent via phone call, email or letter to avoid customers not receiving appropriate information about the extent of their consent or their rights to withdraw consent at any time.

Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	Overall, AIA NZ is concerned that the Bill leaves a great deal of detail to regulations and standards. While each designated industry will have differences that need to be accommodated in standards, to provide greater certainty for participants and consistency across sectors, the Bill should include minimum standards related to certain fundamental requirements such as security and storage of data, and consent. Alternatively, if the Government considers that minimum standards across sectors are not appropriate, at the very least, there should be minimum details that standards *must* address for all designated customer data. This will provide greater certainty to all participants, enabling them to provide meaningful feedback during future consultation and encouraging wider uptake of the CDR regime. In our view clause 88 of the Bill should also specifically require the Chief Executive, before the standards are made, to consult data holders who will be impacted by the standard as a group. We also support a similar amendment to clause 61 to specifically require the Minister to consult with the proposed designated data holders before designation regulations are made. While the Bill provides for consultation with those the Chief Executive or the Minister (as applicable) considers to be substantially affected by the proposed standards or designation regulations (as applicable), in our view any person or entity who could be affected should be included in consultation, especially data holders. AIA NZ considers that data holders that would be subject to proposed standards or designation regulations would always be "substantially affected" by those standards or regulations, and as such, any discretion of the Chief Executive or Minister around consultation with data holders should be removed to avoid ambiguity. Consultation with data holders will be critical to encouraging industry support and ensuring that the standards and regulations are workable in practice. Consultation with data holders could also reduce public sector cost and time spent developing standards and regulations by leveraging industry expertise. Given the significance of standards and the Bill, extensive industry consultation on all standards and adequate transition periods will be essential to ensuring that the standard can be operationalised and that it delivers the policy objectives of the Bill without causing undue impact on data holders' resources which are already focused on customer service.
8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*
	AIA NZ does not think the Bill is clear as to how storage and security requirements interact with the Privacy Act. Consistent with our feedback on other sections of the Bill, it is difficult to assess how the requirements would interact with the Privacy Act because much of the detailed requirements will be set by standards and regulations that are yet to be developed. While the Bill expressly provides that a breach of the CPD storage and security requirements (as defined in the Bill) in relation to personal information will be treated as a breach of an IPP under the Privacy Act, it is unclear what this would mean in practice. If a data holder breached a CPD storage and security requirement in relation to personal information as well as non-personal information, how would this be dealt with by the regulators? AIA NZ does not believe that an MOU between the OPC and MBIE is the appropriate mechanism to resolve these questions. The Bill should address how these issues will be addressed to give participants confidence that there will not be dual-track investigations and create potential double liability. We also consider that the inherent differences between the Privacy Act and the Bill have the potential to drive further complexity and cost into compliance. The Privacy Act is a

deliberately flexible, principles-based statute, whereas standards under the Bill will likely be detailed and prescriptive (for example, like those under the Australian CDR regime). Paragraph 26 of the Discussion Document states that the Bill relies on existing Privacy Act protections and that these are not replicated in the Bill unless:

- the Bill provides the same protection as an IPP but sets a more specific requirement for customer data; or
- an equivalent Privacy Act protection is required in the Bill to ensure consistent treatment of all customer data (whether personal information or not) for simplicity, cost effectiveness and to ensure sensitive commercial information also has protection.

However, the first point is potentially problematic as, by their nature, the IPPs are intended to be flexible. If CDR standards are highly prescriptive, they will be hard to reconcile with the flexible IPPs and will potentially create conflicts between the two regimes.

There are already a number of international standards which set out best practice for the storage and security of customer data. It is our view that these standards would be the most appropriate minimum requirements for the CDR regime to apply as it safeguards customer data in a way that is already well understood by data holders. It is also important that there are not different standards for storage and security depending on the sector.

We are also concerned that clause 48(2) is ambiguous and does not adequately define CPD storage and security requirements, particularly because it is difficult to imagine any regulations made under the Bill which would not be captured by the broad "catch-all" provisions in paragraphs (c) and (d), which cover any regulations related to "providing regulated data services" or "otherwise dealing with designated customer data".

For greater certainty, we recommend that CPD storage and security requirements are required to be expressly identified as such in the relevant regulations, and that the Minister's power to recommend that a requirement is a CPD storage and security requirements if the requirement relates to one or more of the matters currently listed in clause 48(2)(a)-(c).

9	*From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards[1] are suitable for use in other sectors, and which could require significant modification?*

AIA NZ is not familiar with the elements of the Payments NZ API Centre Standards and are unable to comment on the specific elements suitable for use in other sectors.

As a general point, the Government will need to be particularly mindful of the nuances between different sectors when developing standards applicable beyond the banking industry. We note that to date, the consultation process around the CDR regime has focussed heavily on the banking sector and while this makes sense with banking proposed to be the first industry designated under the Bill, there are significant differences between the banking sector and other sectors such as insurance. AIA NZ considers that developing standards (and regulations) for the insurance sector will present unique issues that have not needed to be considered for the banking sector.

For example, the banking sector is highly transactional in nature, with a high frequency of data collection, across relatively standardised categories of data, and largely predictable and common use cases for that data. Conversely, because the insurance industry is much less transactional, it does not collect customer data as frequently (customer data is largely collected at the product purchase stage and then on an ad hoc basis during claims or when

[1] New Zealand API standards to initiate payments and access bank account information. They are based on the UK's Open Banking Implementation Entity standards but tailored for the New Zealand market. Market demand has driven development and led to the creation of bespoke functionality for New Zealand.

	customers are prompted to review data accuracy during renewal). The variation in underwriting rules between insurers also means that categories of data collected are likely to differ between insurers, which will make standardised sharing more difficult. The insurance sector also collects a range of highly sensitive health information which requires greater security and protection along with compliance with the Health Information Privacy Code. We also note that the Payments NZ API standards have been developed over several years, following significant consultation with industry stakeholders. This slow development process is reflective of the complexity involved in developing these standards and is consistent with the experience in Australia and the UK. In both the UK and Australia, there were delays in implementing the technical standards for the banking sector, despite long lead times for roll out and significant consultation. The recent review of the Australian framework recommended a slower approach to the phased roll out of the CDR regime to allow participants time to adapt and ensure good customer experience. Given the complexity involved in standards it is our view that standards are best developed by industry groups or bodies to ensure that they are fit for purpose and receive sufficient input from all stakeholders. At the very least, the Chief Executive should have an express obligation to collaborate and consult with impacted data holders or industry groups during the development of standards. Standards which have not been developed by or in collaboration with impacted industries risk being unworkable and near impossible for those impacted to operationalise.
10	*What risks or issues should the government be aware of, when starting with banking for standard setting? For example, could the high security standards of banking API's create barriers to entry?*
	As we noted in our response to question 9, we are not familiar with the standards being proposed for banking API security and are unable to comment on their appropriateness. However, as we noted in our response to question 8, AIA NZ considers that minimum security standards should be set out in the Bill, with additional requirements for specific sectors prescribed in standards and regulations.
Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*
	AIA NZ disagrees with MBIE's position and thinks that a separate accreditation class for intermediaries under the Bill may be useful. We believe that all recipients of customer data as envisaged under the Bill should be accredited requestors including intermediaries. An accredited requestor should not be permitted to share data obtained from a data holder with a third party unless the customer has expressly consented, and the third party is also accredited. This is fundamental to ensure that customer data is protected and that customers have control over their data. We do not think that the Privacy Act is sufficient to protect customer data shared by an accredited requestor without specific customer consent being obtained given the machine-readable format of the information.
12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	AIA NZ agrees that accredited requestors should have to hold insurance and that the criteria for this insurance should not provide a barrier to entry for accredited requestors. We note that it is increasingly difficult to obtain indemnity insurance and cyber incident insurance and other methods of insurance or safeguards may be necessary to prevent

potential accredited requestors from being excluded because they are unable to obtain insurance.

14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*

AIA NZ thinks that the Bill should include a specific provision requiring accredited requestors to delete customer data after consent is withdrawn.

We note that paragraph 35 of the Discussion Document identifies that, unlike the Australian CDR regime, the Bill does not require participants to ensure that they are able to delete designated customer data upon request by a customer. The Discussion Document implies that the Government considers such a requirement to be inappropriate (as New Zealand does not have a general right of erasure of personal information) and/or IPPs 7 and 9 provide sufficient protection to customers. We do not agree with this assessment.

While MBIE may assume that IPP 9 would require the deletion of this data in most cases where a customer has withdrawn their consent, the flexibility of the Privacy Act and IPP 9 can be leveraged to easily circumvent this expectation. IPP 9 requires that agencies not keep personal information for any longer than is required for purposes for which the information may lawfully be used. While the Privacy Act generally only allows personal information to be used for the purposes for which it was collected (the primary purpose), there are a number of exceptions to this requirement which allows agencies to lawfully use information for secondary purposes. If a customer withdrew their consent but the accredited requestor was able to rely on one of the exceptions under IPP 10 to lawfully use the data for a secondary purpose, they would not be required to delete the customer's data.

We do not believe that customers would expect that an accredited requestor continues to hold their data after consent is withdrawn, and that by enabling accredited requestors to retain designated customer data where it can rely on an exception under IPP 10 to lawfully use the data for a secondary purpose, the Bill undermines its objective of providing customers with greater control over how their data is used and the idea of express, informed and current consent.

In addition, AIA NZ has significant concerns that reciprocal data sharing is not required under the Bill.

This is particularly concerning given the intention for "data" to include derived data, and data derived from derived data. Data holders invest significantly in their systems and processes to undertake various functions and generate data which is largely used to assist data holders with internal decision making. If accredited requestors could access this data then they potentially could benefit from the significant investment of data holders, without recourse for data holders. This in turn could stifle system innovation and investment by data holders which will be a negative outcome for customers and their ability to get value out of their data.

As the Bill does not explicitly cover derived data, we propose that either derived data should be excluded from the CDR regime, or the Bill should expressly allow data holders to charge a reasonable fee to accredited requestors for access to this derived data to address the cost associated with generating this derived data.

Ethical use of data and action initiation

19	*What are your views on the proposed options for ethical requirements for accreditation? Do you agree about requirements to get express consent for de-identification of designated customer data?*

AIA NZ strongly supports ethical requirements being a condition of accreditation to ensure that customer data is used ethically, responsibility and appropriately.

We also agree that customer consent should be specifically obtained by accredited requestors for all uses of customer data including anonymised or pseudonymised uses.

Given the scope of the data that accredited requestors may have access to and the Bill's intention to give customers control of their data, we think that accredited requestors should need explicit consent from customers for all uses of their data.

Although AIA NZ supports option two as an appropriate ethical requirement, it is unclear why this ethical safeguard would be extended to data holders. These ethical protections are proposed on the basis that additional safeguards are appropriate to balance the increased ability, under the Bill, for requestors to transmit and store customer data, including potentially sensitive data. Given that data holders already hold and process the designated customer data and will not be receiving or storing additional data as a result of the Bill (except to the extent they are also an accredited requestor), it is unclear why the ethical safeguards should also apply to data holders. Any general obligation for data holders to obtain customer consent before de-identifying or pseudonymising personal information is more appropriately dealt with as part of a review of the Privacy Act.

Additionally, we think that specific attention should be given to the sharing of customer data by an accredited requestor. Requestors who wish to share designated customer data received from a data holder should only be permitted where a customer has authorised this disclosure, in the same way and subject to the same consent requirements as the original authorisation to request the data from the data holder. This would ensure that customers know who has access to their data and control how it is used and shared. It would also help to address AIA NZ's concern that the Bill does not adequately protect customer data from onwards disclosure by accredited requestors (with the potential for an accredited requestor to essentially operate as an outsourced provider but without the principal receiving data from the outsourced service being required to be accredited as well).

20	*Are there other ways that ethical use of data and action initiation could be guided or required?*

AIA NZ believes that it is appropriate for ethical considerations to be included in standards to ensure that the value of a customer's data is distributed fairly between customers and accredited requestors. As the Discussion Document notes customer data is valuable and this value needs to be appropriately shared between participants and customers (i.e. an authorised requestor should not request more customer data than is needed to provide a service to the customer as this additional data could be used to create value for the accredited requestor which is not shared with the customer).

Preliminary provisions

21	*What is your feedback on the purpose statement?*

AIA NZ agrees with the purpose statement in the Bill. However, we also think that the purpose statement should be amended to provide that the maintenance of security of customer data should prevail over the other objectives. We believe that the protection of customer data should be a fundamental overarching consideration of the Bill.

In addition, we suggest that an additional objective of ensuring that the CDR regime is fair should be included in the purpose statement. The review into Open Banking in Australia included fairness as an objective and we think that fairness to all participants is important to ensure that costs and benefits are fair and encourages use of the CDR regime.

22	*Do you agree with the territorial application? If not, what would you change and why?*

AIA NZ agrees that the test is appropriate as it aligns with the test used in other legislation such as the Companies Act 1993 and the Privacy Act.

	We note that academic commentary[2] has called out that this test is problematic due to the fact that specific analysis is required and the alternative interpretations that have been used by the courts, but this issue is outside the scope of the Bill and Discussion Document.
Regulated data services	
23	*Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?*
	AIA NZ agrees that a valid request should not be able to be declined provided that the consent is valid and the request does not go further than the consent. AIA NZ also agrees with the current drafting of the Bill which would maintain the same circumstances for withholding information as currently provided for under the Privacy Act such as section 49. Personal information held by health and life insurers can include sensitive medical information, including information about third parties (for example, information about policy beneficiaries under a group insurance policy provided to an employer or where there are joint policyholders) and there may be various legitimate reasons for the data holder to withhold this information (such sensitive mental health diagnosis which pose a serious threat to the customers safety).
24	*How do automated data services currently address considerations for refusing access to data, such as on grounds in sections 49 and 57(b) of the Privacy Act?*
	CONFIDENTIAL - Commercially Sensitive Commercial Information
Protections	
25	*Are the proposed record keeping requirements in the draft law well targeted to enabling monitoring and enforcement? Are there more efficient or effective record keeping requirements to this end?*
	AIA NZ does not believe that the Bill is well targeted at monitoring and enforcement. Clause 40 of the Bill places the majority of the record keeping requirements on data holders which is a significant burden. The Bill would effectively require data holders to keep a complete record of the data provided to an accredited requestor. This would significantly increase the amount of data stored by data holders, significantly add to cost, and is not aligned with the data minimisation principle in the Privacy Act. In addition, standards may impose additional record keeping requirements resulting in further uncertainty for data holders and requestors.
26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*
	AIA NZ agrees that data holders and accredited requestors should be required to have and maintain a data policy.

[2] *Carrying on Business in New Zealand: an Uncertain Frontier in a Digital Age* (NZBLQ Vol 27 Dec 2022 1, Kavanagh and Yang)

Administrative matters	
28	*Are the matters listed in clause 60 of the draft law the right balance of matters for the Minister to consider before recommending designation?*
	AIA NZ broadly agrees with the matters listed in clause 60 of the Bill. However, similar to our response to question 7, AIA NZ believes that clause 61 of the Bill should be amended to require the Minister to consult with all proposed designated data holders before designation regulations are made. While the Bill provides for consultation with those persons the Minister considers will be substantially affected by the proposed designation regulations, in our view any person or entity who could be affected should be included in consultation, especially data holders. AIA NZ considers that data holders that would be subject to proposed designation regulations would always be "substantially affected" by those standards or regulations, and as such, any discretion of the Chief Executive or Minister around consultation with data holders should be removed to avoid ambiguity. Consultation with data holders will be critical to encouraging industry support and ensuring that the regulations are workable in practice and have considered the full implications of designation. Consultation with data holders could also reduce public sector cost and time spent developing regulations by leveraging industry expertise.
34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*
	Although it is difficult to comment on the appropriateness of a redress cap without further details, AIA NZ supports requirements allowing for customer refunds or redress, as the risks associated with increased data sharing need to be considered and appropriately addressed to protect customers. AIA NZ also considers that providing a clear mechanism for customers to obtain redress is appropriate.