Financial Services Council NZ

Grow the financial confidence and wellbeing of New Zealanders

Monday 24 July 2023

Consumer Data Right Project Team
Commerce, Consumers and Communications
Ministry of Business, Innovation & Employment
PO Box 1473
Wellington 6140
New Zealand

By email: consumerdataright@mbie.govt.nz

Customer and Product Data Bill Exposure Draft

This submission on the Ministry of Business, Innovation and Employment (MBIE) Unlocking value from our customer data, a draft law to set standards and safeguards for customer and product data exchange, June 2023 (the Discussion Document) and the exposure draft of the Customer and Product Data Bill (the Draft Law) is from the Financial Services Council of New Zealand Incorporated (FSC).

As the voice of the sector, the FSC is a non-profit member organisation with a vision to grow the financial confidence and wellbeing of New Zealanders. FSC members commit to delivering strong consumer outcomes from a professional and sustainable financial services sector. Our 114 members manage funds of more than $95bn and pay out claims of $2.8bn per year (life and health insurance). Members include the major insurers in life, health, disability and income insurance, fund managers, KiwiSaver, and workplace savings schemes (including restricted schemes), professional service providers, and technology providers to the financial services sector.

Our submission has been developed through consultation with FSC members and represents the views of our members and our industry. We acknowledge the time and input of our members in contributing to this submission.

We welcome the opportunity to provide feedback on the Draft Law which brings in a consumer data right (CDR) for New Zealand and respond to the questions in the Discussion Document. Please note we have not included the questions which our members have no comment on at this time.

Our members have concerns that there are challenges with the Draft Law and how this interacts with the Privacy Act 2020 (the Privacy Act) and the Information Privacy Principles (IPPs) creating difficulties in how the Draft Law would be operationalised and compliance costs for organisations. We understand and support the importance of establishing safeguards for customers and their data, however rushing legislation (including details left to regulations and standards) without considering thoroughly the unintended consequences will not best meet these objectives and potentially negatively impact the industry. We strongly encourage further thought and consideration on how the two sit together, prior to the introduction of the Draft Law to Parliament.

We welcome continued discussions and engagement and extend a further invitation to attend the FSC Regulation Committee if this would be helpful Privacy of natural persons

Privacy of natural persons

Yours sincerely

Richard Klipin
Chief Executive Officer
Financial Services Council of New Zealand Incorporated

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?

We consider that overall, the interaction between the Privacy Act and the Draft Law has not been fully appreciated and that there are uncertainties which will make the Draft Law difficult to operationalise. The Privacy Act relies on principles whereas the draft law will contain detailed standards that apply to personal and non-personal information.

We agree that the disapplied sections are appropriate, however it would be helpful to have guidance in respect of some of the IPPs of the Privacy Act. For example, IPP 8, namely the requirement for an agency to ensure information is accurate, up to date and complete before using or disclosing. It would also be of value to gain further clarity around how potential disclosures outside of New Zealand as part of the new CDR will adhere to IPP 12 of the Privacy Act.

Further clarification would also be welcomed on the regulatory oversight for the proposed framework. As proposed, multiple regulators would be responsible for administration, which may lead to inefficiencies and overlap. For example, MBIE and the Privacy Commissioner will both be involved in compliance and enforcement. In our view this will not lead to good customer outcomes as dealing with disputes will be delayed and hard to navigate.

There is also the potential for unintended consequences for organisations due to the disparity between the Draft Law and the Privacy Act. For example, under the Privacy Act organisations keep records of the information provided when requested as evidence of their compliance. The Draft Law could be interpreted as also requiring evidence of non-personal information supplied under the Draft Law to be kept which would create a significant additional burden for organisations. We do not consider this to be the intention of the Draft Law, however the interaction between the Privacy Act and the Draft Law should be more explicitly explained or guidance provided to avoid such unintended consequences.

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

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

We do not consider that there should necessarily be a prescribed maximum. The duration of the consent should be commensurate with the service enabled by that consent, namely, if the customer is seeking a one off comparison or switch and change transaction, the limit of the consent should be relatively contained. However, for ongoing 'live service' offerings, an indefinite term would make sense, albeit it should be justifiable.

Point 60, on page 24 of the Discussion Document states that customers can specify how long an authorisation is for, when they sign out for a product or service. We consider this to be potentially problematic, as a customer would not have any frame of reference to understand what the 'proper' term to select would be. We consider the term of the consent should be disclosed clearly, and available to be viewed by the customer at any time, combined with the conditions relating to the end of the authorisation (as noted in response to Question 4 below). This approach would ensure that ongoing services are not artificially disabled by a customer's lack of understanding, but they are still protected.

In general, customers would not want to take another action following an initial onboarding for services that persist beyond a single transaction. Implementing a specific expiry period would likely cause more customer resistance to such offerings than an incentive.

We note some FSC members do see value in a maximum duration for customer consent to increase customers' engagement and understanding of where and how their data is being shared. These members believe that six months may be an appropriate time frame for consent with a simple reconsent process to reduce the burden of a customer reconsenting.

Therefore, we encourage consideration of different consent periods, and this could also depend on the way in which consent is obtained. For example, when a data holder receives consent directly from a customer the consent should be valid for longer than consent which comes via a data requestor's application. In addition, it may be helpful to have periodic 'push notifications' or reminders sent to individuals outlining which entities they have consented to sharing data with. These notifications could have an active ongoing consent every 12 months with a reminder both of the service utilising their data, but also the process to terminate that consent if no longer relevant. This would enable individuals to revoke consent where they no longer desire the data sharing to be occurring, without setting an arbitrary timeframe of maximum duration.

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

We agree with the circumstances proposed when consent should end. We suggest the inclusion of additional circumstances for authorisation ending to cover when an accredited requestor ceases to be accredited, and when a data holder becomes aware that a customer has died.

In addition to future regulations that will be able to specify events which require authorisation to end, we also support additional powers for the Privacy Commissioner to revoke or suspend a requestor's accreditation. These additional powers or via regulations should also extend to ending or suspending all related data sharing in the event of a significant data breach or where an accredited requestor is found to be in breach of the authorisation requirements.

We disagree that consent should cease upon a customer closing their account as there may be valid reasons why customers' data is useful after account closures, such as for lending applications where historical transaction data may be relevant.

In the event MBIE considers a timeframe is necessary, we consider this would be more appropriately specified by the agency offering the product or service rather than the customer, as the agency is far better placed to advise on the necessary duration for authorisation.

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?

Point 69, on page 26 of the Discussion Document states, "If an accredited requestor receives a withdrawal of consent, they must notify the data holder (and vice versa)". It is not clear why this would be required if the regulatory framework specifies the level of automation and systemisation of these requests. A manual notification process beyond a call to an Application Programming Interface (API) or similar transportation layer would seem to provide only a loophole for data holders to avoid truly implementing the systemisation and technology to support a CDR.

The previous point on page 26 states, "If a customer wishes to withdraw their consent, the consequences (if any) of doing so must be outlined by the accredited requestor or data holder." We consider this intent to be correct, however this wording in the Discussion Document does imply that there may be

consequences other than a degradation or loss of the service enabled by access to the customer's data through the CDR which we consider to be inappropriate.

In addition, we consider the requirement to communicate with customers when consent is given and ends, and when a request is actioned could cause customers to experience notification fatigue. It is unclear whether it is the data holder or the accredited requestor's responsibility to communicate with a customer and in what timeframes. We suggest the Draft Law clearly assign roles and responsibilities for each customer communication and allow for communications to be aggregated.

Care during exchange: standards

7. Do you think the procedural requirements for making standards are appropriate? What else should be considered?

Our members are concerned that the majority of the Draft Law details are left to regulations and standards. Whilst some standards will be industry specific, matters such as security and storage of data, the accreditation criteria and consent will apply universally and as such should be set out in the Draft Law to ensure consistency and certainty for all.

The design of regulations, standards and designations for each sector should be required to consider expected cost and benefit (both in terms of the inclusion of relevant information and features, and the impact of obligations on both small and large data holders in the sector) to ensure they are not unduly burdensome.

We encourage the provision of more certainty in respect of the potential scope of the obligations that may be placed on data holders by regulation, standards and designations and there needs to be appropriate and clearly defined guidance on what is to be taken into account. To ensure that key matters are identified and considered when developing regulations, standards and designations, the Draft Law should include clear timing and process requirements, including statements of intent, clear timetables for consultation and response periods.

We consider the procedural requirements for making standards to be appropriate, however we think that all impacted data holders should be specifically listed as a group that must be consulted. All data holders, regardless of the perceived impact on them, should have the opportunity to provide feedback.

8. Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?

We do not consider the Draft Law is clear as to how storage and security requirements interact with the Privacy Act in all respects. However, as the requirements will be set by standards it is difficult to assess this in more detail at this time. We note that the Privacy Act is a principles based legislation designed to be flexible and that standards under the Draft Law will likely be specific and detailed, creating potential conflicts between the two regimes that will be hard for data holders to reconcile.

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

We note the Payments NZ API standards took several years to develop following significant consultation with stakeholders. All standards under the Draft Law should take a similar collaborative approach to ensure that all operational matters are taken into account to achieve the value desired by the Draft Law.

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?

We note that there are already a number of international standards which set out best practice for the storage and security of customer data. We consider that these standards would be more appropriate standards for the CDR regime to apply as it safeguards customer data as they are already well understood by data holders.

Trust: accreditation of requestors

11. Should there be a class of accreditation for intermediaries? If so, what conditions should apply?

We consider the proposal to allow accredited requestors to share data with other entities if consented to by the customer is appropriate. Specifically barring this sharing and requiring a carve out for intermediaries as per the Australian framework is potentially confusing and limiting.

In addition, any sharing of data by accredited requestors should be specifically consented to as part of a customer's consent and be able to be withdrawn at any time.

Our members have concerns about requirements to provide information to, and open systems to, any other third party that have not been through accreditation and who may not have security measures in place to protect data provided (nor be subject to contractual or legislated requirements in respect of proper use of the data). We also consider a lack of uniform security and privacy standards could result if accreditation is "weakened" and there are not clear requirements to ensure appropriate handling and use of consumer data. Therefore, we suggest that data should not be required to be provided to anyone other than an accredited requestor.

12. Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?

We agree 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. It may also be appropriate that accredited requestors are required to hold cyber insurance.

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

We would like to highlight issues with the proposed accreditation process.

The Draft Law should include a specific provision requiring accredited requestors to delete customer data after consent is withdrawn. We do not consider that customers would expect that an accredited requestor continues to hold their data after consent is withdrawn, but this scenario would be possible under the Privacy Act if the accredited requestor had a lawful purpose to retain the data.

The Draft Law currently proposes that non-accredited third parties (who are not required to comply with the CDR) will be permitted to receive CDR data from accredited requestors, which potentially increases the risks to safety and security significantly and creates a back door to access CDR data whilst avoiding CDR compliance costs, undermining the purpose of the CDR.

The New Zealand regime does not include a principle of reciprocity. If the exchange of consumer data is truly said to enhance competition, then accredited requestors should also be required to make their data available to others, subject to the overriding principle of consumer consent. From a banking perspective,

particular competition risks may result from 'big tech' and other similar entities becoming accredited requestors under the regime.

As proposed, data holders will also be required to mandatorily share customer data direct to customers themselves, who may not be well set up to protect that data and who may on-share to non-accredited third parties outside of the proposed protections of the Draft Law. Whilst this is technically possible under the Competition and Consumer (Consumer Data Right) Rules 2020 in Australia, we note that it has never been permitted on the basis that the benefits to the customer do not outweigh the risks.

Under the Draft Law, non-accredited parties can make requests via the CDR to data holders. Whilst data holders do not have to comply with them, some may choose to do so in circumstances where there is a potential commercial gain.

Unlocking value for all

16. What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?

Fintech providers are considered to have an advantage in this space, acting as distribution intermediaries across all financial sectors, such as a robo advice proposition incorporating a digital advice facility under their Financial Advice Provider license alongside a CDR driven onboarding process. This has the potential to be transformative for providing much wider groups of customers access to high quality financial advice.

The Privacy Act in its current form is too narrow in offering protections for business customers due to its focus on personally identifiable information. This is one reason why the Code of Professional Conduct for Financial Advice Services, which supports the Financial Markets Conduct Act 2013, contains a wider duty to protect client information. We note the definition in the Draft Law of customer means a person, suggesting the protections for a business may not exist as intended. The Privacy Commissioner therefore may not be the appropriate regulatory body for dealing with complaints relating to business customers unless its scope of powers is broadened.

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?

We do not agree with requirements to obtain express consent for de-identification of designated customer data. De-identified data for real customers is considered to be the most effective tool for driving enhanced customer experience and service. The principles based approach governing ethical use of that data is sufficient and this requirement would all but guarantee that no usable insights would be garnered from any customers utilising a CDR enabled service.

Further guidance and clarity on what is considered de-identified data in this context will be required.

Part 2: 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?

We consider this to be appropriate as the only way to truly unlock value from a CDR is if there is no individual decision making or discretion in the application of requests. These must be entirely systemised.

We encourage further clarity and provision for circumstances where data holders may decline requests to provide information and perform actions.

It is important that complying with the obligations imposed on data holders under the Draft Law does not conflict with data holders' obligations under other legislation. Without consideration of this the Draft Law could be unworkable for data holders. For example, complying with the Draft Law could conflict with data holder obligations under AML/CFT legislation, sanctions legislation, cyber-resilience requirements and formation of a view that valid requests are fraudulent or part of a distributed denial-of-service (DDoS) attack.

This issue could potentially be addressed by allowing the data holder to decline to process a request if it forms the view that to do so would be contrary to applicable law. Such other laws should also be explicitly considered when developing regulations, standards and designations.

We note some life and health insurers hold sensitive customer health information for legitimate purposes and that there are valid reasons for not disclosing this information under the Privacy Act. These members agree that the Privacy Act provisions relating to withholding information should apply to the Draft Law but note that these decisions are typically manual which would delay any exchange of information.

Part 5: 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?

We consider section 61 of the Draft Law should be amended to require consultation with all persons or their representatives who will be impacted by the proposed designation. We do not consider the Minister will be able to determine who will be substantially impacted and all those who could be impacted should be given an opportunity to submit.

32. Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?

We consider real time reporting to be preferable.

Complaints and disputes

35. In cases where a data holder or requestor is not already required to be member of a dispute resolution scheme, do you agree that disputes between customers and data holders and/or accredited requestors should be dealt with through existing industry dispute resolution schemes, with the Disputes Tribunal as a backstop? Why or why not?

We suggest further clarification on the disputes resolution scheme, including the role of various regulators in resolving disputes is needed. We also encourage consideration of establishing a specialised dispute resolution scheme in this space.

Other Comments

1. The Privacy Act and its protections are principles based and without a fines regime other than for failing to comply with compliance notices or failing to notify the Commissioner of specific breaches. Whilst there are aspects of the Privacy Act that are appropriate for CDR, there are residual concerns that the Privacy Act may not be fit for purpose in its current form to underpin a New Zealand CDR.

Given the transformative nature of a wide CDR, it would appear to be an ideal opportunity to reform current Privacy law in combination with the introduction of the CDR, including the scope of the Privacy Commissioner's powers.

2. The regime should seek to leverage and align with the work done via the API Centre (for example, the Data Standards, API Standards and security requirements) and other relevant regimes including the Digital Identity Trust Framework that are part of the existing compliance framework in the banking sector.

3. There is overlap of several key pieces of legislation including the Privacy Act and its amendments for personal information. We also note extraterritorial legislation such as the Consumer and Data Standards in Australia (for non-personal information) and the General Data Protection Regulations. We suggest further clarification on how these interact and best practice for New Zealand.

4. We note MBIE's initial view was that only 'provided' or 'observed' data would be subject to the CDR. However, under the Draft Law, 'derived' data (being data that has been created by a data holder through the application of insights and analytics) is included as in-scope of potential designation for mandatory data sharing. This data has been derived by the data holder through proprietary means which may be commercially sensitive. Care needs to be taken to ensure that the regime does not discourage data holders from investing in new data allowing others to free-ride off that investment. The Draft Law should ideally carve out enhanced or enriched data where the data holder has invested in creating something new of value.

   An alternative approach could be for New Zealand to adopt the approach from Australia whereby a delineation is made between mandatory data and voluntary data (derived). Requests for voluntary or derived data could be subject to different thresholds and potentially fees to ensure data requestors (or disruptors) do not attempt to capitalise on this to gain access to competitor proprietary information.

5. Due consideration should be given to safety and security of consumers, especially with the rise of fraud and scams. As data holders, banks will be required to mandatorily share customer data with third party accredited requestors that they have not themselves undertaken any form of due diligence on. Whilst we acknowledge this may be mitigated by the accreditation and consumer consent process, we have concerns that this may not be sufficient to appropriately safeguard our customers against risk.

6. It is important that appropriate friction is built into the system to allow for the appropriate checks to be undertaken. We would like to draw attention to the recent commentary and regulatory change in both Australia and the United Kingdom where changes have been made retrospectively to allow for more time for data holders to check credentials in response to fraud and scams.