24 July 2023

Submission: Draft Exposure Bill on Customer and Product Data

Executive summary

1. Paymark Limited trading as Worldline (**Worldline**) is pleased to submit on the Ministry of Business, Innovation and Employment (**MBIE**) draft exposure Customer and Product Data (**CPD**) Bill (the **Bill**) and discussion document entitled "Unlocking value from our customer data" (the **discussion document**) as published on 29 June 2023.

2. Worldline submitted on this topic in 2020 in response to the "Options for establishing a consumer data right in New Zealand" consultation. We are grateful that many of the matters we raised then have been taken into consideration.

3. In this submission, we provide general feedback on the proposed system for accessing and exchanging data under the Bill. We also respond to MBIE's specific questions in the **attached** Appendix.

4. In summary, we would like to see a supervisory rather than prescriptive regime; one that provides legal certainty in the overarching primary legislation, as to obligations, liability and regulatory oversight, yet is flexible enough, in the secondary legislation, to evolve and change with technological advancements and customer wishes. Where possible, duplication should be limited. In payments, we are already at risk of overlapping accreditation processes, standards, regulators, and legislative regimes. Standards and accreditation frameworks need to be coherent and work in harmony with each other, rather than competing or conflicting. They should be created, and developed, by industry in co-operation and collaboration with MBIE, and there must be a clear mechanism for versioning. For this regime to work, it needs to be sustainable and commercially viable. Lastly, we need uptake. No one will use it if they do not know about it nor trust it. Clear, consistent, educational and reliable communications are vital.

5. Worldline largely endorses the Payments New Zealand (**PNZ**) submissions on the current and previous consultation papers, so far as they relate to the API Centre.

6. We do note that given the short time frame to respond (including a period when staff are on leave during the school holidays and over Matariki weekend), we have not had a chance to thoroughly analyse the impact this Bill will have on our business, our industry, or "NZ Inc". We understand others in our industry are in a similar position. Whilst we appreciate the webinars, and MBIE facilitating a virtual submission session for Fintech NZ and Digital Identity NZ members, there is general concern that the consultation period has not been long enough to gather the feedback required to ensure the Bill is fit-for-purpose. This may result in a higher risk of harmful unintended consequences.

Worldline New Zealand history

7. Worldline New Zealand was established in 1984 to provide low-cost Eftpos transaction processing as a way of enabling banks and merchants to move from cash to electronic payments. We are New Zealand's leading payments innovator, and we design, build and deliver payment solutions that help Kiwis succeed. Worldline New Zealand has been a part of Worldline SA, our parent company (a French corporation), since 2020.

8. We have evolved over time and, whilst we continue to provide payment processing for eftpos transactions, we also process transactions that are routed out to the global card schemes (such as Visa and Mastercard), provide payment gateway solutions to ecommerce platforms and directly to ecommerce merchants, and are leaders in embracing API-based technology for open banking payment services.

9. Over the last 7 years, we have focussed on innovation, investing millions in developing and building a state-of the art API[1]-based payment platform[2] and new local debit payment methods for use both instore and online.[3] We have fully integrated payment APIs with the four largest New Zealand consumer banks and one of the smaller banks. We are a foundation member of Payments New Zealand's API Centre. We are active in both the working and business groups, and until recently, the API Council. As far as we know, we are the only payments company to have a product in market that utilises APIs built to the API Centre's standards for payment APIs.

10. Our key comments in relation to the CPD Bill are as follows:

Clear roles & responsibilities of overlapping regulatory jurisdictions

11. The payments industry is navigating its way through several regulatory initiatives across several different regulators. We consider it vital that the CPD regime be interoperable with other related frameworks; not just the Privacy Act 2020[4] but also the Retail Payments System Act 2022[5] (**RPS Act**), and the Digital Identity Services Trust Framework Act 2023[6] (**DISTF Act**). Given the recent enactment of both the RPS Act and the DISTF Act, there is an opportunity to ensure that they work efficiently with the proposed CDP regime. We would like to see a holistic, overarching strategy be developed in respect of payments (noting that the Reserve Bank of New Zealand (**RBNZ**) is also developing payments-related objectives under its Future of Money[7] initiative).

12. The New Zealand Commerce Commission (**NZCC**) announced that it will be consulting on account-to-account payments later this year.[8] NZCC has indicated that retail payments facilitated by payment service providers utilising APIs will be subject to the RPS Act. Whilst we do not disagree with the sentiment, we would like to understand how the NZCC's roles and responsibilities will interact with MBIE's, and that of the Privacy Commissioner when it comes to open banking payments products. The potential for conflict and overlap is significant and determining which regime takes precedence in the case of conflict could be challenging to navigate.

---

1 Application Programming Interfaces (APIs) work as a highly secure channel, allowing two different systems to safely communicate with each other and share information.

2 See https://www.paymark.co.nz/future/.

3 See https://www.paymark.co.nz/products/online-eftpos/.

4 See https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html.

5 See https://www.legislation.govt.nz/act/public/2022/0021/latest/whole.html.

6 See https://www.legislation.govt.nz/act/public/2023/0013/latest/LMS459583.html.

7 See https://www.rbnz.govt.nz/money-and-cash/future-of-money.

8 See https://comcom.govt.nz/regulated-industries/retail-payment-system.

Utilise already established standards and frameworks

13. Significant investment has been made through PNZ's API Centre for the purpose of payment APIs.[9] It makes sense to leverage off the existing investment made by participants in API Centre work. The API Centre's terms and conditions, and the standards, have been developed with the direct input of industry. Lessons from the API Centre work to date should be learned from and incorporated. Despite varying degrees of readiness,[10] and commitment to implement APIs,[11] most of New Zealand's retail banks have been involved in the API Centre and many of the topics set out in the discussion document have already been considered and worked through.

Mind the gap(s)

14. *Data:* The term "data" is not defined. In the discussion document, "derived data" is intended to be subject to the regime, yet what is meant by "derived data" is unclear. In Australia, a similar proposal was criticised on the basis that it may compromise data holders' proprietary insights. As such, their Consumer Data Right legislation has mechanisms to limit the scope of what "derived" means, and it specifically excludes materially enhanced information.[12] In Worldline's opinion, neither derived data nor data that has been enriched by a data holder using their own internal methods should be included in the CPD regime, particularly if it is protected by existing intellectual property rights. In defining and limiting the scope of "derived data", we need to consider terms such as "raw" or "primary" and "enhanced". All are different and should therefore be treated differently. Furthermore, it is unclear whether the CPD regime would only apply to data produced after the introduction of the regime (forward looking data) or also pre-existing data.

15. *Protecting business data:* We note that personal information is protected by the Privacy Act but how business information is to be protected is not covered in the Bill. We are concerned about the confidentiality and sensitivity of commercial information, which in many cases will include derived data that has been compiled from the primary data of many customers. At worse, the sharing of commercially sensitive information could give rise to competition law, confidentiality, and financial market conduct issues.

16. *Action initiation:* The privacy implications related to customer data requests have been considered but not those related to action initiation. The API Centre has done good work in this space and Worldline recommends considering the approach that they have taken and implemented.

17. *Direct access:* We understand the Bill provides for direct access of customers to data holders however there is little in the way of information about how this will practically take place. We have long hoped that a CPD regime would assist merchants who wish to switch online payment gateways but are disincentivised from doing so because incumbent payment gateways may not agree to the transfer of card tokens to a new provider, or will do so only at significant cost.

---

9 See https://www.apicentre.paymentsnz.co.nz/.

10 See https://www.apicentre.paymentsnz.co.nz/standards/available-standards/api-provider-readiness/

11 See https://www.apicentre.paymentsnz.co.nz/standards/implementation/minimum-open-banking-implementation-plan/

12 See https://www.oaic.gov.au/consumer-data-right/consumer-data-right-legislation,-regulation-and-definitions/consumer-data-right-data

If merchants could request to transfer card tokens to a new provider at no, or a reasonable cost, competition would ensue. However, we cannot see how this scenario is provided for in the Bill. Please note, to avoid confusion with paragraph 14, we would consider card tokens to be primary data, rather than derived data.

18. *Liability:* There is no mention of how liability will flow through the regime. Again, MBIE could leverage the work that has been completed by the API Centre on the responsibilities of participating parties.

19. *Verification and authentication methods:* While it seems obvious that the identity of all entities in the data sharing chain need to be verified, we do not know how this will be done. The number of scams and fraudulent claims by those pretending to be others (whether it be someone pretending to be an individual or a business) are many, varied, and increasing both in frequency and sophistication. For this regime to be successful, New Zealanders will need to trust the system and its processes. Robust digital identity services need to be embedded in the regime. Businesses and consumers both need access to those services and verifiable credentials need to be issued by core agencies, such as the Department of Internal Affairs, Ministry of Transport, Ministry of Health and Ministry of Education, Inland Revenue, as well as data holders.

20. *Reciprocity:* The Bill does not include a reciprocity regime which means that the banks and others caught by the initial designation will be required to make data available to accredited requestors (which could include major corporate players and tech giants), who have no reciprocal obligation to make their own data available. While the lack of reciprocity may increase uptake initially, it could lead to an uneven playing field, making certain data requestors (especially the global tech giants) very powerful. They will have a competitive advantage as they benefit from the regime without having to comply with it themselves.

21. *Screen scraping should be banned:* The discussion document specifically says screen scraping will not be prohibited. However, Worldline firmly believes that payment methods requiring consumers to share their online banking credentials with third parties should not be allowed to operate. These third parties access the bank accounts of others using their login credentials to make money transfers on their behalf. Most banks' terms and conditions prohibit the sharing of these log-in details, yet it still happens. If New Zealand wishes to protect the data of its people, those services which utilise screen scraping methods should be prohibited. The purpose of this legislation to is enable the secure sharing of data. It seems contrary to the purpose to then let unsafe practices continue. If these unsafe methods are allowed to operate, firms may not choose to go through the cost of accreditation when they can simply go around the regime. While we agree that data sharing should be able to take place outside the regime. However, when it comes to the safety and security of people's money, perhaps the riskier services should not be allowed to continue. Australia has recently raised banning screen-scraping under their CDR regime for this very reason. In parallel, we note that POLi have shut down operations in Australia yet they plan continue in New Zealand.[13]

13 See https://view.email.auspost.com.au/?qs=6e7335bf6dd1507355dd0ad3fa74031a10ddeddc1ebf59b0cbe112ac73d5cd69113af0b19f1087b98fdd55498ce88df997c8716893154525d3b7d81a11ab73763fc68f4965d56f70d4d7bcfd2e73e5d5148f82657ccdb5fb and https://www.itnews.com.au/news/australia-post-to-close-poli-payments-597950

Value of accreditation

22. A sensible balance needs to be found as an over onerous accreditation regime could become a barrier to entry. We are not convinced that becoming accredited will remove the need to have bilateral agreements in place with data holders unless the CPD regime has mandatory terms and conditions, including liability, on which access will be provided to accredited requestors.

23. We also acknowledge that, without knowing the criteria by which an application to become an accredited requestor will be approved, nor the standards that are to be met, or whether alternatives will be prohibited, it is difficult to assess whether the costs would undermine the viability of accreditation. We note that being a member of the API Centre incurs costs by way of financial and in-kind contributions.

24. Worldline agrees that a trust mark (or something similar) to identify that a data requestor is accredited would be beneficial. However, we need to know more about how ongoing compliance with accreditation will be managed and how use of the trust mark will be monitored. We would need to know that the trust mark is reliable and who is accountable when the accreditor requester ends up being untrustworthy.

It's complicated

25. Complying with the data exchange standards and accreditation requirements will in themselves be complex from both an operational and a technical perspective, not to mention costly. In addition, the same piece of data could be both within and outside the regime. Data holders and data requestors will have to be set up to deal with two categories of the same data, with separate requirements attaching to each. It would be useful to understand how this can be managed in a cost-effective way.

Intermediaries

26. The use of intermediaries would allow New Zealanders to benefit from consistent rules for data access under shared data infrastructure and governance, as well as reducing implementation costs for data providers and data requestors. We agree that third-party intermediaries need to themselves be accredited to be able to perform key obligations on behalf of other parties.

27. Intermediaries will need a mechanism to ensure the customer has consented to their data passing to the data requestor. Intermediaries and data requestors will need to work together to ensure that consents provided by customers cover the data services provided by the intermediary as well as the data requestor. Intermediaries will need to be able to show that they have the correct consents to enable them to share and use the data. While the consent provisions seem very detailed in the Bill, it is not clear how these will work in the case of intermediaries. If consent has been provided to a data requestor, how does the intermediary ensure it is operating in accordance with that consent, and if the customer revokes or changes its consent, how will that be passed on to the intermediary.

28. Data designated under the CPD regime should somehow be identified as "**CPD Data**" and protected as it goes through an intermediary and on to a data requestor in accordance with customer consent. It is not clear whether once data is with an intermediary, how they themselves could access and used the CPD Data and whether non-accredited parties can access and use the CPD Data – if it is personal information this is protected by the Privacy Act but if it is business data then it is not. Worldline submits that this area needs more

consideration. Allowing non-accredited parties access to CPD Data may result in mistrust of the regime.

Considering consent

29. The consent (authorisation) requirements for joint account holders, as set out in the Bill, are not appropriate for payments. We think that consent should be required from all accountholders, and it is not appropriate to seek or receive consent from only one of the accountholders, unless perhaps the other accountholder has delegated their consent in a way that can be captured. Unfortunately, even that could be problematic from the point of view of protecting vulnerable individuals. We believe it would be best to consult with the banks and their accountholders as to how this could work in a safe way.

30. For payments, customers should be able to give a recurring (or ongoing) consent, should they want to. In our experience, consumers want to be able to provide ongoing consent in relation to:
    - recurring bill payments;
    - for those services currently paid via direct debits; and
    - for purchases made at preferred merchants and are frequented by the shopper.

31. Customers should be able to choose the duration and cancel when they wish. Having to renew your authorisation when you still want the service can be a poor user experience, but on the other hand, it might be challenging to keep track of all the consents you have given over time. Ideally these would be visible within a customer's online banking platform and cancellable from there, similar to how direct debits are managed by banks in the United Kingdom now or how your app subscriptions can be managed via your phone. If there is to be a maximum duration, the regulations would be the best place to deal with that, as it will depend on the risk and use cases in each sector. For Worldline, a 12-month maximum could be acceptable. The API Centre standards on customer consent are a good start.

Quality is key

32. The practical ability to implement a CPD regime needs to take account of providers' existing technology systems and would require significant standardisation to be useful. We are not suggesting the choice or use of technology is regulated, but there does need to be some sort of consistency in respect of data output.

33. To avoid the risk of fragmenting versions and standards undermining standardisation, ongoing lifecycle management is needed. This includes specification of support standards, platform security, fault / incident management, and consequences for when access to CPD goes down due to systems failures. Standards will need to evolve over time to minimise costs and dysfunction through fragmentation and poor lifecycle management.

34. Data platform stability, service levels, and data quality need to be fit-for-purpose and regularly maintained. The data must be reliable and accessible in a consistent format. Data reassurances on first use, and subsequent use, must be attainable.

Commercial Matters

35. Ideally the CPD regime will facilitate increased business efficiency, innovation and transparency, and allow businesses and individuals to have greater choice, flexibility and control over their data. However, the implementation of the CPD regime will also impose costs

on business. We would like assurances that the costs of becoming accredited under the CPD regime would take that into consideration. Furthermore, when it comes to charging for services, we note that many jurisdictions have not seen huge successes after implementing an open banking or open data regime. This is due, in part, to the lack of a sensible commercial model.[14] We need to be wary of 'free of charge' models (such as that implemented in India[15]) as the lack of revenue makes justifying investment decisions difficult and can lead to a stifling of innovation.

36. As mentioned above, non-existent commercial models, or those directed entirely by regulation, have meant that the anticipated benefits of open banking have not yet been realised. Despite our best efforts, it is already challenging to move incumbents in the payments industry to new payment products and networks, largely due to the financial incentives associated with the interchange fee model attached to Visa and Mastercard products. The interchange model might be rational for individual decision-makers at issuing banks, but it results in sub-optimal or inefficient outcomes for New Zealanders collectively. The rapidly increasing proportion of scheme cards in use, along with increase in surcharging, means that Visa and Mastercard products are by far the most accepted by merchants for payments in New Zealand. "NZ Inc" should be wary of becoming beholden to the schemes for its payment products and the associated processing system.

37. We do agree that limitations on the prices charged by data holders need to be considered. However, the technology used to make the CPD Data available needs to be reliable and have high availability. For that to happen, the data holder needs to be incentivised (either via regulatory or rational means). If a service isn't always available, and the data quality is poor, it could lead to a bad customer experience and limit the opportunities for innovative, real-time products to be developed.

38. In time, sectors designated under the CPD regime will be economy-wide and many of them already highly regulated. We would like reassurance that MBIE is considering this and is, where possible, minimising the uncompensated and avoidable costs of compliance and participation in the CPD regime.

Conclusion

Worldline is grateful for the opportunity to submit on the draft exposure CPD Bill. We are excited to be a part of what should become a thriving open data network. We would like to work together, within our industry, and across others to truly unlock the value of data for New Zealand consumers and business. We hope further consultations, in respect of regulations and standards, will be given the time and attention needed to be fit-for-purpose. We welcome the opportunity to work collaboratively and cooperatively with MBIE to assist in delivering on the overarching objective; to promote competition and innovation for the long-term benefit of customers.

Should you wish to discuss any of the points raised in this submission, please contact Julia Nicol.

---

[14] https://openapi.ulsterbank.co.uk/bankofapis/v1.0/dynamic-content/content/assets/community-articles/Open_Banking_Report_Final.pdf

[15] https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/DPSSDISCUSSIONPAPER5E016622B2D3444A9F294D07234059AA.PDF

Worldline 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?*
	It is sensible to rely on what is already in the Privacy Act and the disapplied portions seem to make sense. Worldline is concerned that there may be some confusion over who is subject to what, and when, in the case of intermediaries and/or outsourced providers. We are interested to understand more about how the roles and responsibilities between MBIE and the Office of the Privacy Commissioner will be shared and how the different enforcement regimes will be applied. We also are not clear, given much of the detail will be in the regulations, how the storage, security and transfer processes, and requirements will interact between the obligations in the CPD Bill and the Privacy Act. Worldline also submits that the Privacy Act should be reviewed to ensure it continues to the fit-for-purpose and is sufficiently robust. For more information, see paragraphs 11, 12 and 16.
Consent settings: respecting and protecting customers' authority over their data	
2	*Should there be a maximum duration for customer consent? What conditions should apply?*
	Customers should be able to choose the duration and cancel when they wish. It is not a great customer experience to have to renew when you still want the service, but on the other hand, it might be challenging to keep track of all the consents you have given over time. If there is to be a maximum duration, the regulations would be the best place to deal with that as it will depend on the risk and use cases in each sector. For Worldline, a 12-month maximum could be acceptable. The API Centre standards on customer consent are a good start. For payments, consumers should be able to give a recurring consent, should they want to. In our experience, consumers want to be able to provide ongoing consent in relation to: • recurring bill payments; • for those services currently paid via direct debits; and • for purchases made at preferred merchants frequented by the shopper. Please also refer to paragraphs 29, 30 and 31 on consent.
3	*What settings for managing ongoing consent best align with data governance tikanga?*
	Participants will need to be guided by good principles. To ensure that this is the case, we could benefit from having access to guidelines that are tailored to this CPD regime, such as those published by Stats NZ.[16]
4	*Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*

[16] https://data.govt.nz/assets/data-ethics/Nga-Tikanga/Nga-Tikanga-Paihere-Guidelines-December-2020.pdf

	Worldline agrees with s 31 of the draft Bill, however we think accredited requestors should be able to revoke consents if there is some security risk, scam, fraud or illegitimate data use by a customer. Worldline also thinks that vulnerable people's interests should be protected. See also paragraph 31.
5	*How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?*
	No comment.
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?*
	The consent requirements set out in the draft Bill relating to joint account holders are not fit-for-purpose when it comes to payments. Ideally all those named as account holders should approve a payment prior to it being made, especially if it has a high value. There may however be some way of delegating consent, but we expect that this might breach their bank account terms and conditions and would need to make sure that vulnerable people were adequately protected. See also paragraph 29.
Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	Industry created standards that evolve would be ideal but how will the engagement be facilitated? See also, paragraphs 4, 13, 25 and 33.
8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*
	Given that we do not yet know what the storage and security requirements under the CPD Bill will be, it is difficult to comment on the interaction between them and the requirements under the Privacy Act. There also appears to be a gap in respect of business and product information which is not personal information and therefore not covered by the Privacy Act. This can be sensitive and risks can arise if it is freely shared. Competition law and commercial confidentiality are areas that may need to be considered in respect of business or product information.
9	*From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards[17] are suitable for use in other sectors, and which could require significant modification?*

[17] 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.

	No comment, as Worldline is not familiar with other sectors. More generally, and for efficiency reasons, existing industry standards and certifications should be considered. To the extent possible, MBIE should look to re-use these rather than duplicate time, cost and effort in creating new standards and/or accreditation criteria.
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?*
	Security standards must be high when it comes to payments.
Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*
	Yes, for those that store and/or pass-through information. Intermediaries should be required to disclose how they use and store data that has been received under the CPD Regime. If the data is stored by an intermediary, that data should retain its designation as CPD Data. See also paragraphs 26, 27 and 28.
12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	Yes, public and products liability including professional indemnity. In respect of the banking sector, MBIE may wish to utilise work already completed by the API Centre in respect of insurance.
13	*What accreditation criteria are most important to support the participation of Māori in the regime?*
	Worldline cannot speak for Māori but we would like to see: • clear and transparent communications published by Government around the risks and benefits of the regime; • trusted advisors across sectors, communities, hapu, iwi and whanau explaining and educating businesses and consumers, and promoting the regime; and • Te Ao Māori approaches to data governance embedded in the CPD regime by design, not as an after-thought.
14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*
	Accreditation should not just be in respect of the data requestor being fit and proper but that the use case for which the data is being requested is robust. Each service/use case should itself be accredited alongside the data requestor as a company.
Unlocking value for all	

15	*Please provide feedback on:* • *the potential relationships between the Bill safeguards and tikanga, and Te Tiriti/the Treaty* • *the types of use-cases for customer data or action initiation which are of particular interest to iwi/Māori* • *any specific aspirations for use and handling of customer and product data within iwi/hapū/Māori organisations, Te Whata etc, which could benefit from the draft law.*
	No comment.
16	*What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?*
	Worldline does not think specific use cases should be designed, as it is more likely to create unintentional barriers or blockers to use cases that have not yet been considered. The legislation should be use-case agnostic and provide for good practice, risk reduction, etc. What would, however, be useful is to include designs for verified information including fraud check for high value purchases, verified address and verified age check.
17	*What settings in the draft law or regulations should be included to support accessibility and inclusion?*
	Collaboration with representatives of vulnerable consumers should take place from the start and their expertise should be considered and incorporated. We note that some good work has been done in respect to this by the payments industry in Australia: https://www.auspaynet.com.au/accessibility
18	*In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?*
	The CPD legislation should be drafted in a way so as to ensure compliance with this upcoming legislation https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/accessibility/making-aotearoa-accessible/index.html. The only concern Worldline has is that the accessibility legislation in progress may be watered down during the parliamentary process making it challenging to achieve its overriding objective of driving accessibility and inclusiveness.
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 should look to the European General Data Protection Regulation, where if data is de-identified in a way that the data subject is no longer identifiable, then consent to use that information is not necessary.[18] Once information has been depersonalised, it should no longer fall within the regime.
20	*Are there other ways that ethical use of data and action initiation could be guided or required?*
	The process should be easily accessible, safe and comprehensible for disabled people, vulnerable people and people who may have difficulty understanding what they are initiating.
Preliminary provisions	
21	*What is your feedback on the purpose statement?*
	No comment.
22	*Do you agree with the territorial application? If not, what would you change and why?*
	Yes, although we note that similar provisions in the Companies Act and the Privacy Act are not without their challenges. Some of the biggest global data holders and intermediaries (for example, Facebook, Google, Amazon, WeChat, Alipay) may be able to find ways around being subject to the regime.
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?*
	No. Data holders should be able to decline a request for security or fraud reasons, in line with current practices for banking services.
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?*
	No comment – not applicable to Worldline.
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?*
	These are acceptable.
26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*

[18] https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

	Worldline believes that including a requirement to describe which checks are carried out before using an outsourced provider would create unnecessary work for little benefit. We consider that derived data should not be included in the regime nor be included in the definition of CPD Data, as it may be challenging to link the derived data back to the data originally shared under the regime. The customer should be informed about intermediaries and whether an intermediary stores the information or passes the information through.
Regulatory and enforcement matters	
27	*Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?*
	No.
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?*
	The following items should be considered: • The benefits to customers • Whether the attributes of the sector giving rise to requirements related to intermediaries should be accredited and if data held by the intermediaries should be subject to the designation
29	*What is your feedback on the proposed approach to meeting Te Tiriti o Waitangi/Treaty of Waitangi obligations in relation to decision-making by Ministers and officials?*
	At Worldline, we do not have tikanga experts who have knowledge of Te Ao Māori approaches to data governance, so we would like to have access to the experts or be reassured by the experts that the approach set out in the draft Bill meets the Te Tiriti o Waitangi/Treaty of Waitangi obligations. Worldline would prefer that, not only the decision-making process was compliant but that the Te Ao Māori approach to data governance was embedded into the CPD regime, so it is incorporated by design, into any data that is identified as CPD Data and shared in accordance with the legislation (once enacted).
30	*What should the closed register for data holders and accredited requestors contain to be of most use to participants?*
	• In the case of data holders; the data they hold • In the case of accredited requestors; the use case for the data and related consent framework/scope • Assurance of quality • Risk management processes • Security controls and potentially any standards they follow • Certification

31	*Which additional information in the closed register should be machine-readable?*
	Some sort of “certificate” or “token" issued to accredited requestors that people can verify and vice versa.
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?*
	It is acceptable for Worldline. However, it may be preferrable to determine the dates in regulations so that other reporting obligations applicable to those operating within a certain sector are not all happening at the same time.
33	*Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?*
	It depends on the use cases attached to the APIs. It also depends on what is meant by real-time reporting. It is difficult to determine if this means being able to access the performance data at the time you want to request it or being able to access a data feed that is always updated in real time. We note that real time is practically almost impossible when it comes to reporting and suggest that the term “near real time” is used instead.
34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*
	Determining whether a cap should be included in regulations, and if so, what amount it should be, will depend on the industry designated and use cases of the accredited requestors. We would not want a cap to leave customers without an adequate remedy. If a cap is not high enough, people will not trust the system.
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?*
	Worldline has been active in open banking payments since 2016 and has not required an industry dispute resolution scheme, nor has any claim made its way to the Disputes Tribunal. What sorts of claims are anticipated under this regime? Misuse of personal data should go via the Office of the Privacy Commissioner, noting that we do have concerns those processes and rights of redress may not be sufficiently robust, and the Privacy Act likely needs updating to provide greater protection for consumers. Misuse of business data may be covered by other areas of law, e.g. Competition Law or Finance Market Conduct prohibitions, but the route to enforcement would need to be clear, simple to use, and cost-effective in each case. As banking is the first designated sector, it could make sense for customers to be able to use the Banking Ombudsman. Rather than setting up new dispute resolution schemes, it would be more efficient if those already in place could be utilised.