Status quo and problem definition	
1.	What are your experiences of accessing consumer and product data for electricity under the status quo?
	We do not have a view on this point.
2.	Do you agree with our summation of the status quo and problem definition? Is anything missing or incorrect in your view? And please provide any evidence you may have to support your views.
	We do not have a view on this point.
3.	Do you think that regulatory options are necessary to unlock better access to customer and product data?
	We do not have a view on this point.
4.	What do you consider to be the likely outcomes for access to customer and product data in the absence of a CDR for electricity?
	We do not have a view on this point.
What a consumer data right for electricity could look like	
5.	Who else may be impacted by a designation of the electricity sector? Should particular groups or classes of entities be explicitly included or excluded from a potential designation?
	We want to emphasise that electricity data, especially from smart meters, can be highly detailed and may include personal information about other individuals at the premises, such as tenants, family members, or employees, whose behaviour can be inferred through data analysis.
6.	What customer data do you think is the most important? And what else (now or in the future) would be important? And why? What are the benefits from consumers having ready access to this data?
	From a privacy perspective, any information about an identifiable individual is considered personal information. As such, this data requires protection under the Privacy Act 2020. Further, it is recognised that when personal information attracts a reasonable expectation of privacy, it may be afforded special protection, such as under privacy torts. This is particularly relevant to electricity data from smart meters, which can potentially reveal household behaviors (as noted in *R v Alsford* [2017] NZSC 17).

	In Aotearoa, according to the Electricity Authority, smart meters currently have 90% coverage. We believe that the data potentially collected by smart meters is crucial, as it enables new business opportunities but also introduces significant privacy risks.
7.	If access to customer data is designated for all consumers (residential, small business, large business and large consumers) what are the potential benefits, risks or costs associated with each type of customer? And why?
	Consumption data from smart meters not only reveals the electricity usage of the account holder but also allows for granular monitoring that can infer consumer habits, preferences, usage patterns, and general household behavior. This includes personal information about others in the household, such as tenants, family members, or employees. Therefore, clear guidelines on access, use, and sharing of this data should be established, with specific rules on consumer consent and limitations when sharing information with third parties. The Privacy Commissioner has stated that "usage data," once linked to an individual account holder, constitutes personal information (Case Note 251185 [2015] NZ PrivCmr 3). Additionally, the ability to collect more data through advanced technology does not grant third parties or energy companies unrestricted access. Data collection should be limited to purposes explicitly authorised by consumers. It is also important for data users to recognise that historical data is only reliable when consumer behaviour is consistent over time. Otherwise, decisions based on this data may result in inaccurate predictions and negative outcomes for consumers.
8.	What product data do you think is the most important? And what else (now or in the future) could be important? And why? What are the benefits from this data?
	We do not have a view on this point.
9.	Are there any other issues with product data we should be aware of? And why? Please provide examples.
	We do not have a view on this point.
10.	What factors should be considered when identifying who the best data holder is under a potential CDR regime? And how might contracting agreements affect the application of a CDR in regard to data holders? (e.g., contracts between metering equipment providers and retailers to share data).
	Determining the most appropriate entity to act as a data holder will clarify the responsibilities of all participants under the forthcoming Customer and Product Data Act and the Privacy Act 2020, particularly regarding statutory obligations like handling data access requests and accountability for data breaches. A key factor to consider is whether personal information is processed for the entity's own purpose/goal or on behalf of another. If the processing is done for the entity's own

	purpose—such as providing a service—under the Privacy Act 2020, the agency is fully liable to meet privacy obligations (see e.g. s 11, Privacy Act 2020). It appears that regardless of who collects the data, retailers have access to it and use it for their own purposes, which means they should always be designated. Additionally, if metering equipment providers (MEPs) use data for their own purposes, they should also be designated. However, if the data life cycle (collection, use, deletion, destruction) is managed by an entity acting on behalf of the principal agency (following instructions), that entity is likely already under contractual obligations to the principal agency. In such cases, there may be no need to designate that entity, as they do not have any independent purposes or uses for customer data.
11.	Do you agree with our initial framework for how to identify/designate data holders? Why or why not?
	We do not have a view on this point.
12.	What actions could be designated for electricity under a CDR? And why? What are the potential benefits from these? Please provide examples.
	We do not have a view on this point.
Potential benefits and risks	
13.	What are your thoughts on the potential impacts of a designation on the interests of consumers? Are there any specific benefits that are likely to be enabled with designation? What is the likely scale of the benefits, and over what timeframe would they occur?
	We do not have a view on this point.
14.	Do you have any comments on the specific interests of different types of consumers, such as, residential, business, industrial, rural, Māori, or other groups of consumers?
	Different types of customers typically have privacy interests in their electricity data, as its use can infringe on their privacy (see the response to question 17 for more detail on risks). This does not apply to business customers, whose privacy interests are not recognised in New Zealand. However, electricity data from any customer is likely to contain information about other individuals at the premises, such as tenants, family members, or employees. The exchange of such data poses privacy risks to all these individuals.

	We believe that consumers recognise the value of their data, not only to themselves but also to organisations offering products and services. To minimise privacy risks, they expect the electricity system to be secure, reliable, and to provide practical control over their data—such as through customer dashboards.
15.	What are your views on the nature and scale of costs/benefits? Who would these costs/benefits apply to and when?
	We do not have a view on this point.
16.	Would you be able to quantify potential additional costs to your organisation associated with designation under the Bill?
	We do not have a view on this point.
17.	Do you have any comments on the benefits and risks to security, privacy, confidentiality, or other sensitivity or customer data and product data?
	Below are some potential risks and vulnerabilities associated with customer data containing personal information: **Risk of surveillance and profiling** Smart meter data can be used to build detailed profiles by tracking household energy usage. With two-way communication enabled by smart meters, the risks are amplified as data is both collected and transmitted externally. This can effectively turn homes into spaces under surveillance. The data could also lead to negative outcomes such as discrimination, misuse of personal data, or unsolicited targeted marketing. Therefore, it is crucial to protect smart meter data from commercial misuse by third parties who may infringe on the privacy of customers and other household members. **Risk of intrusion into personal life** The household is traditionally viewed as a private space. However, with the granularity of smart meter data, it may be possible to infer real-time activities within the home, providing detailed insights into individual habits throughout the day. While smart meters and homes bring advancements in electricity management and efficiency, these technologies can become intrusive without clear boundaries. The absence of privacy by design and default in the smart grid system can harm individuals by violating their reasonable expectation of privacy and intruding on their personal affairs. **Risk of identity theft** The collection of personal information from customers can lead to identity theft or impersonation, as well as issues with authentication. Electricity companies are generally seen as secure environments for storing and verifying personal information. However, a leak or the unauthorised sale of data from these companies could expose customers to these risks. **Risk of discrimination or exclusion from services**

	Consumers may face retaliatory actions for making decisions such as switching service providers. We are of the opinion that such retaliatory action should be clearly prohibited by the designation regulations. Additionally, there is a risk of discrimination against consumers who cannot access new technology, such as in areas without smart meters, limiting their ability to benefit from more advanced services. **Cybersecurity Risks** The energy sector is critical infrastructure, and disruptions—whether physical or cyber—can severely impact the supply of electricity services. Cybersecurity risks extend to connected smart meters, with potential threats such as unauthorised firmware updates that could control or manipulate household devices linked to the smart grid. In an interconnected system, a breach at any point could affect the entire network, creating a domino effect that impacts everyone.
18.	Are there any risks from the designation to intellectual property rights in relation to customer data or product data?
	The designation should aim to strike the right balance between privacy interests and intellectual property interests. In our view, customer data should not be limited to information that customers can access through their electricity providers. As technology evolves, opportunities to generate **derived data**—by combining various data sources to make inferences and decisions about individuals—are increasing. This derived data, often created by extrapolating from existing customer data along with other inputs (including opinions, inferences, and potentially inaccurate information), may include details unknown to the customer or information they would not have willingly disclosed (e.g., false opinions). Such data is also used by organisations to tailor products and services to customers. We believe that derived data should be included in the scope of designation. Accredited requestors and/or data holders may generate derived data incorporating customer information, and it should not be processed without the customer's consent or outside their control. Since derived data related to an individual is considered personal information, it can have the same impact as direct customer data, potentially leading to harm if mishandled.
Other aspects of a potential designation	
19.	What do you consider to be important if designing an accreditation regime for the sector?
	We believe that **customer confidence** is of a central importance to the success of the Ministry objectives. That means it is essential that the scheme has **privacy and trust** built into every aspect of its design. That trust, which encourages customers to engage with accredited requestors and with the whole system, should be fostered not merely by the system's convenience and reliability, but by ensuring that privacy is one of the main considerations. Key factors are the need to: - minimise data sharing risks; - offer clear and standardised consent mechanisms; and - ensure responsible handling of customers' data and robust and user-friendly enforcement mechanisms that safeguard customer data and protect customers from potential harms. Those harms include not only financial loss or identity theft, but also damage to dignity and/or autonomy of customers (e.g., exposure of behavioural profiles

	of a customer). It is essential that the designation regulations not only minimise risks for customers (see the list of risks in the response to question 17 above) but also ensure appropriate responses when these risks materialise. For example, if a data holder experiences a notifiable privacy breach, the regulations should stipulate that their accreditation is suspended pending an investigation. Accreditation should only be reinstated once any necessary remedial actions, as required by the Ministry and/or the Privacy Commissioner, have been completed. In our view, serious failures in risk management—such as failing to notify a privacy breach as legally required by the Privacy Act—should generally lead to suspension and potentially the cancellation of accreditation.
20.	What are your views on fees for requests for customer electricity data under the Bill? If fees are charged, what limits or restrictions should be placed on fees? Do you have any comments on the costs and benefits of the various options?
	We believe that future data holders, given their market position and the advantages of scale, are well-positioned to provide these services free of charge. Any charges, if applied, should not be based on data holders' initial infrastructure investments, as this would unfairly burden new market entrants with the cost of recouping those investments. Additionally, the Ministry should ensure that inefficiencies in data holders' costs are not passed on to new entrants. In other words, any fees should be based on efficient, long-run incremental costs. We also note that under the Privacy Act 2020 (see s 66), private sector agencies may only impose charges for making information available or providing assistance, and all such charges must be reasonable.
21.	Are there any particular considerations for electricity that should be taken into account for a consumer consenting process?
	We view customer consent as a critical element in ensuring that individuals maintain control over their data and in fostering trust. We note that the consultation document uses the term "consent," where the Bill uses "authorisation." Individuals need assurance that their personal information (e.g., detailed electricity information describing their behavioural patterns) is well-protected, and that if their choice of an accredited requestor proves to be a mistake, they can withdraw their authorisation and request the erasure of their data, including any downstream data held by secondary users or third parties. This minimises the risk of harm from the use of their data. To be valid, authorisation/consent should be: - intentional, - informed, - specific (which could be included under informed), and - free from controlling influence. For consent to be informed and specific, the authorisation request must clearly identify the customer data, the purposes for which authorisation is sought, the intended recipients of the data, and the purposes for which the data may be used under that authorisation.

	The requirement for consent to be intentional means that the customer must explicitly confirm their desire to participate. Authorisation should not be assumed, for example, as part of general terms and conditions. This also means that consent must be "opt-in." Customers should separately agree to the use of data necessary for providing the service and to any additional uses of the data that are not essential. This ensures that the customer truly agrees to those additional uses, without bundling consent into a single line that covers additional risks that the customer is unaware of. Additionally, the customer should not only be informed about the subject matter requiring authorisation but also about the authorisation process itself. Customers should be informed about the duration for which the authorisation is active and how to revoke it if they wish to do so.
22.	Do you think that standards should be led by industry, by government or co-led? What is the role of industry in developing standards? And why?
	We do not have a view on this point.
23.	How do you believe a CDR and the Code could/could not work together?
	We do not have a view on this point.

General Comments:

Thank you for the opportunity to make a submission on the proposed regulations.

Privacy Foundation New Zealand supports the designation's goals of facilitating competition, enabling innovation, and promoting secure, standardised, and efficient data services. We encourage the Ministry to consider our proposals above to find the best path to foster customer trust and encourage the swift uptake of these services.

About the Privacy Foundation
The Privacy Foundation New Zealand Inc was established in 2016 to protect New Zealanders' privacy rights, by means of research, awareness, education, the highlighting of privacy risks in all forms of technology and practices, and through campaigning for appropriate laws and regulations. Its membership has a diverse range of professional, academic and consumer backgrounds and the Foundation regularly lends its collective expertise to comment on proposed regulation or programmes in the media or by participating in consultation processes.

This submission was prepared on behalf of the Privacy Foundation New Zealand by Maria Tenorio and Dr Marcin Betkier from the Foundation's Privacy in the Digital Economy Working Group.

Thank you

We appreciate you sharing your thoughts with us. Please find all instructions for how to return this form to us on the first page.