Consumer Care Obligations - Privacy Impact Assessment (PIA)

1. Purpose

1.1. This paper identifies and assesses the key privacy risks associated with the Authority's *Consumer Care Obligations* project.

2. Project Summary

2.1. The Authority has amended the Electricity Industry Participation Code 2010 (the Code) to:

(a) enhance protections for residential consumers, especially for medically dependent consumers or for those facing hardship, and

(b) provide clear, practical, and enforceable obligations on electricity retailers, improving transparency and accountability.

2.2. The amendments to the Code will mandate the current voluntary Consumer Care Guidelines that were introduced in 2021.

2.3. The amendments will come into force in two tranches. Tranche 1 will take effect from 1 January 2025 and will provide two key protections:

(a) prohibit retailers from disconnecting customers they know to be medically dependent and impose reporting obligations on retailers if a disconnection occurs, and

(b) require any fees or charges to be reasonable.

2.4. Tranche 2 will take effect from 1 April 2025 and apply to the remaining protections and obligations. Tranche 2 includes requirements on retailers to provide information and reporting to the Authority. Collectively, the new Code provisions are referred to in this paper as the Consumer Care Obligations.

2.5. The Authority's function under the Electricity Industry Act 2010 to investigate and enforce compliance with the Code will extend to the new Consumer Care Obligations.

2.6. In the course of performing its functions, the Authority and its agents will receive personal information from or about natural persons who are consumers. For example, a person who is medically dependent may contact the Authority to raise a concern about how they have been treated by a retailer, which will result in personal information – some of which may be sensitive - being disclosed to the Authority.

2.7. The Authority is developing new functionality for its Compliance Portal and website to record and manage information from or about consumers. The Authority is also developing systems and processes for the sharing of personal information with its outsourced call centre (Answer Services Limited), and with the energy complaints scheme provider (Utilities Disputes Limited).

2.8. The Authority has competed this PIA for the project to assess its compliance with the Privacy Act 2020.

3. Assessment of potential privacy risks

3.1. The potential privacy impacts resulting from the project have been analysed against the 13 Information Privacy Principles (IPPs) in section 22 of the Privacy Act 2020, and are detailed in **Appendix A**.

3.2. In summary, the two key privacy risks that have been identified arise from the following activities:

(a) **IPP5 (Storage and security):** the transfer of personal information via email, which may occur when the Authority is communicating with the consumer, retailer, call centre (Answer Services Limited), or the energy scheme provider (Utilities Disputes Limited);

(b) **IPP11 (Transfer to 3rd party):** the failure to obtain consent from the consumer before sharing personal information with a third party.

3.3. The Privacy Team has made recommendations in **Appendix A** to mitigate these risks, primarily through enhancements to the Authority's systems, processes and training.

3.4. The IPPs are a principles-based framework, and this means that there is no rigid approach to compliance. The IPPs generally rely on what is reasonable in the circumstances, having regard to the nature of the personal information, the risk of harm to the individual, and the size of the organisation holding the information.

3.5. This version of the Privacy Impact Assessment represents the Authority's Privacy Team's opinion at the date of publication and will be reviewed and adjusted as necessary as the project develops.

3.6. The Office of the Privacy Commissioner (OPC) has previously advised the Authority in relation to other projects on the importance of reviewing privacy risks over time and keeping the related mitigants up to date. The Authority will therefore update this Privacy Impact Assessment prior to the additional Tranche 2 requirements taking effect.

3.7. OPC reviewed this PIA in December 2024. OPC's only additional recommendation was that the Authority consider an action or implementation plan to take the mitigations listed in **Appendix A** forward and check them off. The Authority will do this as part of the steps described in paragraphs 3.5 and 3.6 above.

4. Attachments

4.1. The following appendices are attached:

- Appendix A Information Privacy Principles - Risk and Mitigation Table

Appendix A Information Privacy Principles - Risk and Mitigation Table

IPPs	Summary of principle	Unmitigated risk	Analysis	Recommended privacy mitigations	Risk after mitigation
IPP1	Do not collect more information than is needed	Yes	The project is proposing to collect the minimum amount of information from consumers (or their representatives) that is necessary to carry out an initial triage of the consumer's concern. The project has developed a form that will be available on the Authority's public website and will also be used by Authority's call centre staff who receive phone calls via its 0800 line. *Self-assessment* The webform contains an initial "Concern self-assessment" step that asks the following questions, and does not require any personal information to be submitted: • "Is your concern related to the Consumer Care Obligations?" • "Has your concern been addressed by your retailer, UDL or another organisation?" • "Do you still want to notify the Electricity Authority" *Notification* The webform requires the following information from anyone that wants to notify the Authority of a concern (with mandatory information marked *): • Name*	**Recommendation**: Privacy Team to update this privacy impact assessment for the Tranche 2 changes that are due to come into effect from 1 April 2025.	No

			• Phone number*
			• Email*
			• If completing on behalf of someone else:
			  ○ Account holder name*
			  ○ Account holder phone
			  ○ relationship with the account holder
			  ○ Permission from account holder*
			• Address*
			• Retailer
			• Concern
			  ○ Type*
			  ○ Date*
			  ○ Description* (max 1000 characters)
			  ○ Outcome of discussion with retailer, UDL, CAB, or other
			• Upload bills, correspondence, photos (max 10 files)
			
			The Privacy Team has discussed this form with the Project Team and is comfortable that the form is not collecting more information than needed for the purpose.
			
			If the Authority determines that further information is required to perform its compliance function then the Authority will collect information in accordance with the Electricity Industry (Enforcement) Regulations 2010 and its relevant compliance and enforcement policies.		

IPP2	Information should be collected directly from the individual concerned	Yes	Personal information will be primarily collected from the consumer directly, either by phone, email or webform. Where a representative of the consumer contacts the Authority, the notification form requires	**Recommendation**: Project Team to ensure the privacy permission forms require consumer consent for any sharing of information between the Authority, Utilities Disputes Limited, and/or the Retailer.	No

	unless an exception applies.		confirmation that the representative is authorised to act on the consumer's behalf (as detailed in relation to IPP1 above). Where the consumer (or their authorised representative) has provided information to Utilities Disputes Limited, the consumer must give consent before this information can be shared with the Authority (and vice versa). If the Authority determines that further information is required to perform its compliance function – such as contacting the relevant retailer - then the Authority will collect information in accordance with the Electricity Industry (Enforcement) Regulations 2010 and its relevant compliance and enforcement policies.	**Recommendation**: Project Team to ensure the Authority's process includes verification of a third party's authorisation to act on behalf of the consumer.	
IPP3	The person collecting the information must be transparent about what they are collecting for and who they will disclose to	Yes	As set out in relation to IPP1 and IPP2 above, consumers may contact the Authority directly to report a potential breach of the Consumer Care Obligations. The Authority will collect the minimum amount of information necessary in order to decide what further action (if any) to take. The Authority anticipates that some consumer queries will be unrelated to the Authority or its role, or may be dealt with more effectively by the retailer or Utilities Disputes Limited. The Authority will seek consent before sharing information to the consumer's retailer or Utilities Disputes Limited.	**Recommendation**: Project Team to ensure the Authority's website and privacy notice is updated to reflect the Customer Care Obligations.	No
IPP4	Information must be collected in a way that is fair and reasonable in the	Yes	As set out in relation to IPP1 above, the mandatory personal information being collected is limited to that needed for the Authority to perform its statutory functions of monitoring, compliance and enforcement. All other information is provided by consent.	**Recommendation:** Project Team to ensure call centre staff are trained and processes are in place for handling calls from consumers where sensitive personal information is being requested or provided.	No

	circumstances and not unreasonably intrusive.		The way that information is collected is through a variety of channels that the consumer can choose, depending on their preference (phone or online). Given the sensitivity of some personal information (eg. medically dependent consumer), there is the potential for consumers to feel that the information requested by the Authority is unnecessarily intrusive. The Authority has engaged Answer Services Limited in recognition of the importance that staff dealing with consumers are appropriately trained. The Authority is developing call centre scripts for Answer Services to use, and training will be provided to all call centre staff.		
IPP5	Storage and Security must be adequate especially for sensitive information	Yes	Compliance with this principle is particularly important given the high likelihood of collecting sensitive personal information such as medical status, consumption information and debt information. *Privacy breach* There are potential privacy breach risks with the transfer of any personal information via email to and between the outsourced call centre, Utilities Disputes Limited and the Authority. Risks also arise where a copy of the information is being sent to the consumer via email. For example, human error may result in email addresses being entered incorrectly, resulting in a privacy breach. To manage this risk in respect of the call centre, the intended solution is for the call centre to be provided access to the Authority's system to directly input the details of a call into the template form. To further minimise the risk of a privacy breach, the call centre will not email the consumer directly with a copy of the form.	**Recommendation:** Manager Data Products to implement and use information transfer solutions that minimise the use of email for personal information. **Recommendation**: CISO to review the Authority's Information policies and procedures at least every 18 months to ensure they are up to date and of good quality. **Recommendation**: CISO to conduct staff training on the updated policies and procedures and continue training on an ongoing basis. **Recommendation**: CISO to audit compliance with the policies and procedures, and who is accessing personal information in the compliance portal. **Recommendation**: Results of the external security review to be considered by the Manager Data Products and GM Corporate and Market Services so that appropriate measures are in place. **Recommendation**: Privacy Officer and Manager Risk and Information Services to run a practice to prepare for a serious privacy/cyber attack.	Yes

			The government model contract in place with the call centre requires compliance with the Authority's policies and procedures that have been notified to the call centre, and with the confidentiality requirements in the contract. *Security breach* With such a large collection of personal information a security breach or cyberattack would be extremely serious, with the potential to cause significant harm. Privacy commentary in Westlaw's *A-Z of NZ Law* provides a suggested framework of measures for agencies holding personal information: (a) regular information risk assessments; (b) establish a culture of security awareness within the agency, including regular cyber security training and testing; (c) develop security policies by consideration to the type of information stored and the sensitivity of that information. The Data Products team have recently completed security hardening measures and also updated their policies and procedures. The Privacy Team recommended that the policies and procedures are reviewed and updated regularly to ensure they are up to date and of good quality. There should also be a staff training programme rolled out together with some auditing of compliance with the policies and procedures. The Data Products team have procured an external specialist to assess the Authority's IT		

			architecture and cyber security systems to check that they are set up to securely store large volumes of sensitive information. The results of the assessment should be considered by the Privacy Team and at Senior Leadership level. The Data Products team also engaged an independent information security auditor to carry out security testing of the system, the results of which determine that the system meets all requisite security standards. Internally within the Authority it is recommended that access to information is on a need-to-know basis. The Privacy Team recommend introducing more formal procedures (to be included in policies and procedures) for staff seeking access to compliance cases involving Consumer Care Obligations. Usage should be reviewed with the Privacy Team every six-twelve months to check that the Authority is compliant with IPP5, IPP10 and IPP11.		
IPP6	Access to information	No	The number of requests by consumers (or their representatives) for access to their information may increase for the Authority. The Authority previously intended that the call centre would, by default, proactively email a copy of the consumer's submission back to the consumer, shortly after receiving the information. This would enable the consumer to check their information is correct, request any changes, and retain a copy for their records. However, given the risk of an inadvertent privacy breach through the use of email, the Authority has changed its process to only email a copy of the submission to the consumer upon request.	**Recommendation**: Privacy Officer to review the policies and procedures for responding to privacy requests.	No

IPP7	Correction of information	No	As above for IPP6, consumers can obtain a copy of their submission from the Authority and request a correction of any personal information held about them.	**Recommendation**: Privacy Officer to review the policies and procedures for responding to privacy requests.	No
IPP8	Accuracy of information must be checked before using or disclosing	No	The Authority must not use information without taking steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading. Any subsequent investigation will comply with the Authority's compliance and enforcement policies, including natural justice requirements to allow the investigated party (eg. a retailer) to be provided with, and have the opportunity to respond to, any factual allegations.	**Recommendation**: Project Team to ensure the information collection processes include a step of providing a copy of the submission to the consumer.	
IPP9	Do not retain for longer than is reasonable in the circumstances	Yes	The Compliance Team require records to be retained for a period of 7 years to comply with the Public Records Act. This is important to enable reviews and investigations to identify systemic non-compliance by any retailers of Consumer Care Obligations. The Monitoring team would ideally like to retain information for 10-15 years to allow for analysis of trends over a reasonable period and support future policy reviews of the Consumer Care Obligations. The Authority should also have systems in place to make sure that personal information is deleted at the end of the retention period (or archived, if the information falls within scope of the Authority's archiving obligations).	**Recommendation**: Manager Data Products, in consultation with the Privacy Team and the Manager Risk and Information Services to review existing procedures (including the Retention and Disposal Schedule) and ensure that a process for disposal or archiving of the information collected under the notice is in place within 2 years of the data being ingested. The policy should identify where personal information can either be deleted or can be pseudonymised, and the identifiers kept secure and separate to better protect the personal information. If we decide a unique identifier is required in relation to any pseudonymisation this PIA will need to be updated in relation to IPP13.	

IPP10	Only use the personal information for the purpose it was collected for	No	The Authority will use the information for the purposes of its monitoring, compliance and enforcement functions relating to the Consumer Care Obligations. The Authority recently updated its Information Management Policy (2024) that sets out the purposes for which information may be used (see paragraphs 3.13-3.17).	**Recommendation**: Compliance Manager (or equivalent) to ensure compliance team understand the purpose of collection and steps required before any investigation or enforcement action taken.	
IPP11	Disclosure to third parties only allowed in certain circumstances	Yes	The Authority's Information Management Policy (2024) notes that the Authority may disclose personal information to third parties, such as government agencies, but only if permitted under the Privacy Act (see paragraph 3.29). As explained in relation to IPP1-3, the Authority will seek consent from the consumer before sharing information with the consumer's retailer or Utilities Disputes Limited. Alternatively, or if the consumer does not consent, the Authority will encourage the consumer to directly contact their retailer or Utilities Disputes Limited. To mitigate the risk of personal information being shared with UDL without consent, the Authority's system requires the privacy consent form to be accepted by the consumer before staff are able to share this with UDL. This reduces the risk of information being accidently released without consent. The Monitoring Team currently only plan to publish analysis, reports or "work product" in an anonymised form which would not reveal an individual. There is some risk of human error though, and this would be reduced by introducing a peer/manager review process.	**Recommendation**: Project Team to ensure the privacy permission forms require consumer consent for any sharing of information between the Authority, Utilities Disputes Limited, and/or the Retailer. **Recommendation**: Manager Data Products, working in conjunction with the CISO, to update information policies and procedures to ensure that the Monitoring Team's published reports have a robust quality assurance process, eg, peer/manager review to ensure compliance.	No

IPP12	Transfer overseas permitted provided certain conditions are met	No	The Authority uses Azure cloud services. Microsoft terms and conditions for Azure cloud storage (including the data protection addendum) adequately reflects the Authority's key privacy obligations in this context. There is room for the terms to be strengthened to better align with privacy obligations but there is limited scope for negotiating those terms.	**Recommendations**: Changes to Microsoft terms and conditions should be reviewed by the Privacy Officer. **Recommendations**: Any change of cloud storage provider to be consulted on with the Privacy Officer.	No
IPP13	Unique identifier not to be assigned to individual unless certain conditions are met	No	Not applicable. This principle does not apply as the Authority will not be assigning a unique identifier to any individual who raises a concern under these Obligations.	**N/A**	N/A