ELECTRICITY AUTHORITY
TE MANA HIKO

Improving retail market monitoring: Privacy impact assessment

Improving retail market monitoring: Privacy impact assessment

1. Purpose

1.1. This paper identifies and assesses the key privacy risks associated with the Authority's *Improving retail market monitoring* project.

2. Project Summary

2.1. The Authority is seeking to improve its monitoring of the retail market and retail market outcomes for domestic and small business consumers.

2.2. There is some information about the retail market and related outcomes being collected by the Authority already but it is not comprehensive, uses a variety of mechanisms (voluntary and mandatory) and there is minimal analysis and reporting. Stakeholders and participants agree that more is required, especially with the amendment of the Authority's statutory objective to include an additional objective to protect the interests of domestic and small business consumers in their dealings with participants in relation to their electricity supply.

2.3. The *Improving retail market monitoring* project is proposing to issue a new standing, mandatory, information request to retailers using clause 2.16 of the Electricity Industry Participation Code 2010 (notice). The notice will replace some of the existing mechanisms, eliminate overlap and uncertainty within the existing requests and, being mandatory, will elicit a more reliable and complete set of data for analysis. It is expected that participants would prefer statutory acquisition rather than being required to provide the information voluntarily as this will ensure they are compliant with Information Privacy Principle 11 in the Privacy Act 2020 (Privacy Act), and obtain some legal protections.

2.4. The notice is requesting information in a different way (i.e. raw data that can be subsequently manipulated) and looks to gather a lot more information than before, some of which is sensitive such as consumption information, medical status debt information.

2.5. Clause 2.16 requires the Authority to consult with impacted participants (i.e. retailers). The Authority is also interested in feedback from other interested parties, including the Office of the Privacy Commissioner, Consumer NZ, consumer representatives and Ministry of Business Industry and Employment.

2.6. The Authority intends to publish metrics developed with data from this notice in monitoring reports such as the quarterly reports and electricity market information (EMI) website.

3. Assessment of potential privacy risks

3.1. A significant amount of the information the Authority is requesting under the proposed new information request is at an ICP level (ie, household level). Within the Authority, it may be possible to link ICP level data to an identifiable individual or group of individuals.

3.2. It is impractical to distinguish between the information relating to natural persons and corporations so, accordingly, the Authority intends to treat all ICP level information received under this request as personal information to ensure consumers are afforded the protections set out in the Privacy Act. This is particularly the case for sensitive personal information like medical status, arrears and half hourly consumption data.

3.3. The Privacy Team's advice about the privacy implications of the notice, including a detailed assessment against the information privacy principles was provided to the Project Team in September 2023 (version 1). 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.

3.4. Since receiving the Privacy Team's advice in September, the Project Team have been progressing the recommendations to ensure the Authority is in a position to responsibly receive large volumes of personal information.

3.5. The key privacy risks identified by the Privacy Team were also highlighted in paragraphs 6.67 – 6.85 of the consultation paper published in December 2023, for industry and interested parties to comment on.

3.6. Submitters broadly agreed with the Privacy Team's analysis of the key privacy risks. Some submitters raised concerns about how the Authority will respond to Official Information Act requests and the costs associated with updating their privacy policies. These comments will be addressed in the Project Team's final decision paper.

3.7. The Office of the Privacy Commissioner (OPC) made a submission (published on the Authority's project page) agreeing that:

(a) the information collected under the notice needed to be treated as personal information

(b) the scale of the proposed collection was "huge", referring to it as "economy wide"

(c) the project created serious privacy risks, but that they could be kept proportional to the policy benefits if the Authority resources and applies "a full range of privacy mitigations".

3.8. The OPC also suggested further attention to the risk of re-identification, given the technological advances happening, and that the Authority consider further mitigants such as steps to prevent onward use of personal information. The Privacy Team have accordingly added recommendations to review policies and procedures more frequently than originally proposed in September, to ensure a structured staff training programme for the Authority's Monitoring Team and Data and Information Management Team is set up and monitored by the Senior Leadership Team. The training programme should include external training to keep staff abreast of technological changes. There is also a recommendation to embed privacy impact assessments into the Authority's processes more formally. Although the Authority does not intend to disclose personal information outside the Authority at the moment, vigilance will need to be maintained over time.

3.9. 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.

3.10. The OPC noted the importance of reviewing privacy risks over time and keeping the related mitigants up to date. The Authority will accordingly put systems in place to ensure that this Privacy Impact Assessment is updated at least every six months (if the notice is progressed) for at least two years from ingestion of data.

3.11. It is recommended that a link to the Privacy Impact Assessment current at the time of publication of the second consultation paper be included in the consultation pack so that interested parties can understand the Authority's approach.

4. Attachments

4.1. The following appendices are attached:

- Appendix A Risk and Mitigation Table

Appendix A Risk and Mitigation Table

IPP	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 the collection of significant amounts of personal information (a combination of raw data and responses to questions) from retailers. This represents a major step change for the Authority. The information will include sensitive information not previously collected by the Authority eg, consumption information, financial information and whether a consumer is medically dependent. The Project Team believe the information is needed for the Authority to fulfil its statutory monitoring functions. The Authority has previously focused its monitoring primarily on the wholesale markets. The Authority's new focus on small consumers (noting that it was given an additional objective in 2022) has highlighted the need to expand and develop its monitoring of the retail market and outcomes for small consumers. Stakeholders and consumer groups have advised the Authority that they think it should collect more information too. The difficulty with applying the data minimisation principle in a data collection process seeking information to support insights across large sectors of the economy is that it can be difficult to find a balance between seeking as much information as needed to provide an in-depth understanding of	**Recommendation**: Project sponsors to oversee execution of the enhanced retail market monitoring work. This should continue for at least two years. **Recommendation**: The Privacy Officer to refresh this privacy impact assessment every six months. Two years from ingestion this could reduce to annual reviews.	No

			the market and the impact of retailer behaviour on consumers, and collecting only the minimum amount of data. Following consultation on the first version of the notice the Project Team have checked that each field in the notice is needed for their intended purpose and can't be easily obtained from another source. Some fields have been removed or simplified as a result. The Privacy Team have discussed this work with the Project Team and are comfortable that the updated notice is not collecting more information than needed for the purpose. Some submitters commented that data is being collected in advance of there being a specific research question to answer. The approach proposed with this notice differs from the previous approach to information gathering. Previously the Authority would use information gathering mechanisms to obtain answers to specific questions. This new approach seeks to obtain a broad base of raw data which can subsequently be used for research and analysis purposes. Different fields can be overlaid upon each other to identify trends and insights. Many specific questions can be answered when needed without issuing a new request eg how many medically dependent consumers are on fixed term plans, or are in arrears. Collecting the data now, in a comprehensive manner, is intended to reduce the need for future information requests. The Privacy Team is satisfied that collecting raw data for the purpose of monitoring, given the broad nature of the Authority's monitoring functions, is reasonable.		

			Importantly though: a) this assessment must be regularly revisited. Circumstances change and it may be that, over time, the purpose does not justify the collection of some or all of the personal information. b) the Project Team must ensure they use the information for the purpose proposed ie ensure resourcing and time allocated and that the proposed monitoring work is executed as planned.		
IPP2	Information should be collected directly from the individual concerned unless an exception applies.	No	It is not necessary for an agency to comply with this requirement if "compliance is not reasonably practicable in the circumstances". In this case it is not reasonable for the Authority to collect this information directly from small consumers as it does not have a relationship with them. Section 24 of the Privacy Act would also apply given the notice is being issued in accordance with the Authority's powers under the Code. Section 24(2) provides that an action taken by an agency does not breach IPP 2 if the action is authorised under New Zealand law.		No
IPP3	The person collecting the information must be transparent about what they are collecting for and who they will disclose to	No	This requirement does not apply to the Authority as it is not collecting information directly. The Ministry of Justice has introduced the Privacy Amendment Bill (Bill) to parliament, and it is expected to broaden the notification requirements under the Privacy Act 2020. It will affect any agency that collects personal information indirectly through other agencies (including the Authority) however the requirements are not expected to apply until 1 June 2025.	**Recommendation**: The Privacy Officer to update the Project Team once the Select Committee reports on the Privacy Amendment Bill. **Recommendation**: The Privacy Officer to update its privacy statement with more information about its statutory information gathering regime.	No

			The Privacy Team will consider the Bill more thoroughly once the Select Committee issues its report (expected November 2024) and advise of next steps. It is likely that the information collected under the notice will be exempt from the notification requirements. Whilst there is not legal requirement to notify consumers of the data collection proposed, the Authority could still encourage retailers to update their policies with a link to the Authority's privacy statement at their next update. If the Authority wishes to use the information for any other purpose eg,market facilitation the Authority will need to conduct a new privacy impact assessment.		
IPP4	Information must be collected in a way that is fair and reasonable in the circumstances and not unreasonably intrusive.	No	There is no particular IPP4 risk identified. The data covered in the notice is a mix of personal information and non-personal information collected by the retailer in the ordinary course of providing electricity services.		None
IPP5	Storage and Security must be adequate especially for sensitive information	Yes	Compliance with this principle is particularly important given the notice proposes collecting sensitive personal information such as medical status, consumption information and debt information. With such a large collection of personal information a security breach or cyberattack would	**Recommendation**: Chief Information Security Officer (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.	Yes

			be extremely serious, with the potential to cause significant harm. The NZ Privacy Commissioner has recently issued guidance about what steps are reasonable to ensure that information held by agencies is kept safe and secure. Information can be found on their website. Privacy commentary in Westlaw's *A-Z of NZ Law* also 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 and Information 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.	**Recommendation**: CISO to audit compliance with the policies and procedures, and who is accessing personal information in the Delta Lakehouse. **Recommendation**: Results of the external security review to be considered by the CISO and applicable General Manager so that appropriate measures are in place. **Recommendation**: Privacy Officer and Manager Risk and Assurance to run a practice to prepare for a serious privacy/cyber attack.	

			The Data and Information Management Team, working with the Authority's Operational Risk and Assurance Manager, 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. 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 the clause 2.16 information held in the Delta Lakehouse. 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	Individuals may have greater awareness of how their information is being used if retailers update their privacy statements. The number of requests for access to information may increase for the Authority. The increase is not expected to be large however given the Authority does not have the direct relationship with the individuals - they will likely contact the retailer in the first instance. Before ingestion the Privacy Team will review its procedures to assess whether any amendments or extra resources are needed to prepare for a larger number of requests and the increased volume of data.	**Recommendation**: Privacy Officer to review the policies and procedures for responding to information requests before ingestion.	No

IPP7	Correction of information	No	As above for IPP6 the Authority is prepared to respond to requests by individuals to correct any personal information held about them however it will review its procedures to assess whether any amendments are needed to prepare for the larger number of requests and increased volume of data.	**Recommendation**: Privacy Officer to review the policies and procedures for responding to information requests before ingestion.	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. In this case the analysis and reports being produced are high level and focused on trends – it is accordingly not reasonable to expect the Authority to check the data in these circumstances. Any analysis and reports will include appropriate disclaimers. If the Authority uses the information "in the course of making a decision to appoint an investigator" as allowed under clause 2.16(3) it should consult with the Legal Team.	**Recommendation**: Manager Monitoring Team to add appropriate disclaimers to work product. **Recommendation**: The Privacy Officer to train Compliance Team on using accurate and complete information.	
IPP9	Do not retain for longer than is reasonable in the circumstances	Yes	The Monitoring team would ideally like to retain information for 10-15 years to allow for analysis of trends over a reasonable period. The Privacy Team consider there to be a good argument that this is a reasonable retention period provided steps are taken to pseudonymise the information as much as possible. 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 and Information Management Team, in consultation with the Manager Monitoring Team, to introduce pseudonymisation of information in the Delta Lakehouse as much as reasonably possible and update the information policies and procedures to reflect the new procedures. **Recommendation**: Manager Data and Information Management Team, in consultation with the Privacy Team 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.	

IPP10	Only use the personal information for the purpose it was collected for	No	The Authority is only allowed to use the information for the following reasons: • to monitor compliance with the Act, the regulations, and the Code • to undertake, and monitor, the operation and effectiveness of market-facilitation measures • to undertake industry and market monitoring, and carry out and make publicly available reviews, studies, and inquiries into any matter relating to the electricity industry The Delta Lakehouse will have strict access controls. The Monitoring Team will be allowed relatively free access to personal information within the Delta Lakehouse for research purposes whereas all other staff will not have access. The Monitoring Team will need special training to ensure they understand the limits for which it can be used. The Compliance Team need training so they understand the limitations set out in clause 2.16(3) of the Code ie: "*the Authority may not specify information under subclause (1) for the purpose of investigating or enforcing compliance with the Act, the regulations and the Code except that it may use information obtained under a notice published under subclause in the course of making a decision to appoint an investigator under regulation 12 of the*	**Recommendation**: Privacy Officer to create a structured staff training programme specifically for the Authority's Monitoring Team before gaining access to personal information in the Delta Lake. This should be repeated every 12 months with an assessment needing to be passed at the end of training. New joiners must be assessed before gaining access. **Recommendation**: Manager Data and Information Management Team (in consultation with the Privacy Officer) will review Monitoring Team's access logs every 6-12 months to assess usage and compliance. (see IPP5) **Recommendation**: Privacy Officer to create a structured staff training programme specifically for the Authority's Compliance Team to ensure they understand the purpose of collection and steps required before any investigation or enforcement action taken.	

			Electricity Industry (Enforcement) Regulations 2010."		
IPP11	Disclosure to third parties only allowed in certain circumstances	Yes	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. The Monitoring Team could also benefit from specialist privacy training to ensure they are vigilant about re-identification risk. They should also be expected to stay up to date with advances in technology. If disclosure is contemplated by staff using the information for market facilitation or compliance purposes, then this would need to be discussed with the Privacy Team. Stats NZ may acquire data from the Authority using their powers in the Data and Statistics Act 2022. They are entitled to use the data to create official statistics, and to add it to the Integrated Data Infrastructure for public interest research. If this happens the Privacy Team will request a privacy impact assessment from Stats NZ and work with them to reduce any risk.	**Recommendation**: Manager Data and Information Management Team to update Information policies to ensure that the Monitoring Team's published reports or "work product" have a robust quality assurance process eg, peer/manager review to ensure compliance. **Recommendation**: Privacy Officer to create a structured staff training programme specifically for the Authority's Monitoring and Data and Information Management teams, with results monitored by the Senior Leadership Team. The training programme should include external training to keep staff abreast of technological changes. **Recommendation**: GM LMC and the Privacy Officer to formally embed a requirement for privacy impact assessments into the Authority's processes. Although the Authority does not intend to disclose personal information outside the Authority at the moment, vigilance will need to be maintained over time as new policy and projects are introduced.	No
IPP12	Transfer overseas permitted provided certain	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	**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

	conditions are met		privacy obligations but there is limited scope for negotiating those terms.		