Australian Government
The Treasury

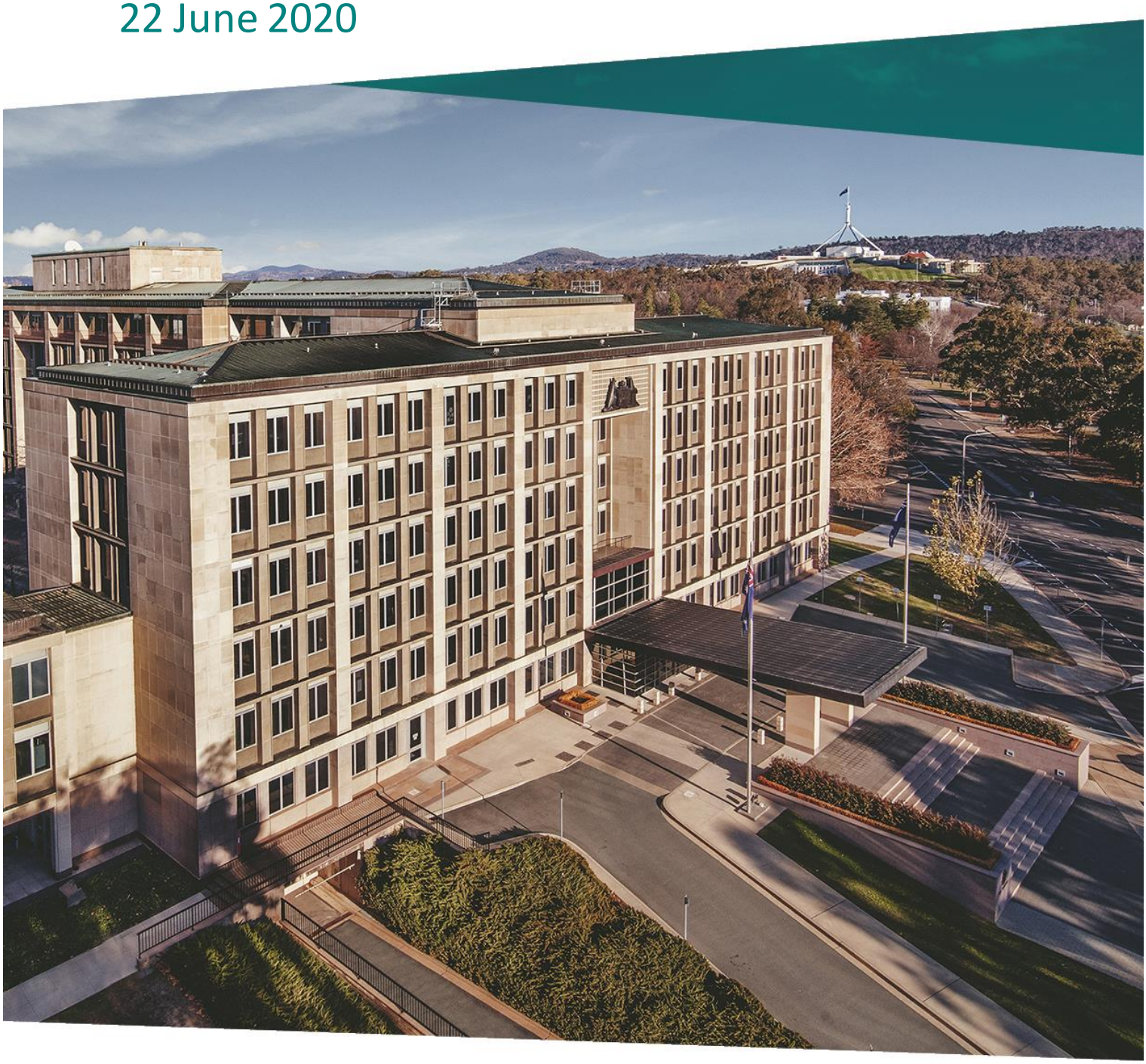
TSY/AU

Consumer Data Right Energy Privacy Impact Assessment

Agency Response

Treasury, Australian Competition and Consumer Commission, Office of the Australian Information Commissioner, Data61

22 June 2020



Manager
Media and Speeches Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

Context

This document has been prepared by the agencies responsible for the design and implementation of the Consumer Data Right in the Energy Sector. It is intended to respond to the recommendations provided by KPMG in their 25 May 2020 Privacy Impact Assessment prepared in relation to the Treasurer's consideration of whether to designate the Energy Sector under s56AC of the *Competition and Consumer Act 2010*.

KPMG recommendation 1 – Further updates to this Supplementary Privacy Impact Assessment (SPIA)

Our assessment and analysis has been undertaken at a point in time in relation to the development of the Consumer Data Right[1], the phased introduction of Open Banking and the proposed designation of Consumer Data Right in the energy sector. Noting that the SPIA has been conducted at this early stage of the designation process, we recommend that it is revisited and that the risks identified and recommendations made are reviewed once the energy rules framework in the Consumer Data Right Rules have been developed, the scope of the Priority Energy Datasets are settled, further consultation has occurred with stakeholders, the authentication model process is agreed, and a PIA in relation to the Gateway (including the data transmission technology) has been completed.

Agency Response: Support

Consideration of privacy risks, through avenues such as Privacy Impact Assessments (PIA) and consultation processes with stakeholders will be ongoing.

Assessments of privacy impacts are mandated for all changes to sectoral designation instruments (s56AD of the *Competition and Consumer Act 2010 (the Act)*) or rules (s56BP of the Act). This is irrespective of the significance of the changes.

The extent to which review of these changes will occur through the creation or revision of a PIA will depend upon the potential significance of the impact. Agencies will rely on the principles and criteria in the Office of the Australian Information Commissioner (OAIC) *Guide to Undertaking Privacy Impact Assessments*, to determine when a threshold is met. While the Privacy (Australian Government Agencies – Governance) Code 2017 legally compels agencies to conduct PIAs in certain circumstances, Consumer Data Right agencies will adhere to the lower thresholds for conducting PIAs set out in the OAIC guidelines.

Regular reviews are proposed for the regime as a whole, including in relation to its privacy impacts. The first holistic review, scheduled by July 2022, is required by s56GH of the Act.

Other ways in which limited privacy health checks may occur (other than through formal PIA processes) include behavioural research into consumer consent processes and independent information security reviews.

Further information on our commitments to conducting PIAs and our treatment of all PIAs as living documents can be found in the earlier *Privacy Impact Assessment – Consumer Data Right, 1 March 2019*.

See also our response to **Recommendation 8**.

[1] Where abbreviations were used in the recommendations, for clarity we have amended the text of the recommendations to include the full term. The recommendations otherwise remain unaltered.

KPMG recommendation 2 – The Gateway

We recommend that a PIA be conducted on the proposed platform and systems that may be used for the Gateway with the involvement of Australian Energy Market Operator (AEMO), Treasury, the Australian Competition and Consumer Commission (ACCC), the OAIC and the Data Standards Board (DSB). We understand that the AEMO is intending to conduct a PIA in due course once it has progressed its own research and consultation and is clearer about the features and obligations of the Gateway. This review will need to consider the pathways in and out of the Gateway.

We recommend that the rules framework for the Gateway should make it clear that the AEMO's handling of the Priority Energy Datasets for which it will not be a Data Holder, will be transient in relation to the data that will be disclosed to an Accredited Person by a Data Holder (such as an Electricity Retailer) through the Gateway. Consistent with the Act, the rules should otherwise restrict the AEMO from collecting and holding or otherwise accessing and using these datasets, save in limited circumstances to support the transfer of data to Data Holders and in other circumstances when exceptions are identified during consultations.

We also recommend that the Consumer Data Right Privacy Safeguard Guidelines are reviewed and updated once the rules for and elements of the Gateway are finalised and a PIA has been undertaken in relation to it, in consultation with the OAIC. These guidelines should promote a further understanding of how the Consumer Data Right Privacy Safeguards and the Australian Privacy Principles will interact and apply to the Gateway in light of its role and the Consumer Data Right Data that it transmits / flows through it and which it collects and holds.

Agency response: Support

Recommendation 2A:

Agencies are working together to deliver a data access model and gateway that ensures data transmitted or held by the gateway is secure and treated in accordance with acceptable privacy practices.

The design of the gateway will be set out in the rules. This will include rules on what and how data flows through the gateway, how it can be used by the gateway, how authentication and authorisation processes work, how it is kept secure, and how various rights granted by the Consumer Data Right regime may be exercised (e.g. deletion rights). Assessments of privacy impacts are mandated for all changes to the Consumer Data Right rules (s56BP of the Act). A supplementary PIA will be conducted prior to the Consumer Data Right Energy rules being made. The AEMO will contribute to this PIA process.

Separately there will be information security assessments conducted regarding the build and proposed operation of the gateway.

Recommendation 2B:

The ACCC is supportive of the recommendation to make clear rules relating to the handling of all datasets by the AEMO in its capacity as the Gateway. The ACCC will consult on this issue through a proposed energy rules framework options paper. We note that subsection 56BG(3) of the Act does not allow the ACCC to create rules enabling AEMO to expand its role beyond what is necessary to act as a designated gateway in Consumer Data Right Energy.

Recommendation 2C:

The OAIC will review and update the Consumer Data Right Privacy Safeguard Guidelines at regular intervals, and particularly following any changes to the Consumer Data Right legislative/rules framework, to ensure that the Guidelines remain current and provide regulated entities with

appropriate guidance. The OAIC will also develop other pieces of guidance for Consumer Data Right entities from time to time, where a need for guidance on a particular topic is identified.

KPMG recommendation 3 – Matters for the energy rules to address

Having regard to the objective of a consistent and interoperable Consumer Data Right framework, the energy-specific Consumer Data Right rules that are being developed will need to address the unique characteristics of the energy sector and how: energy data flows, the AEMO Gateway Model operates, the Priority Energy Datasets are defined and how electricity consumers engage with Electricity Retailers. These rules will need to establish appropriate controls to manage data flowing through the Gateway and allocate responsibilities between Data Holders and Accredited Persons, supported by appropriate changes to the Consumer Data Right Privacy Safeguard Guidelines, Consumer Data Standards, CX Standards and CX Guidelines.

We recommend that, to the extent not already addressed by the Consumer Data Right Rules, the energy-specific Consumer Data Right rules will need to address matters including:

i. allowing authorised representatives of the primary account holder to make Consumer Data Requests;

ii. requiring Data Holders to notify the Gateway and Accredited Person when the Consumer Data Right Consumer is no longer an Eligible Consumer Data Right Consumer, and when the Consumer Data Right Consumer became an Eligible Consumer Data Right Consumer;

iii. review of Consumer Data Right Rule 4.12(3)(b), or development of an equivalent rule tailored for the energy sector, in light of the circumstances in the energy sector where the Consumer Data Right Consumer may not be the individual or the only individual occupying the property to the which the Consumer Data Request relates;

iv. consistent with the current data transfer arrangements, certain data sets that would be considered to be more sensitive, such as Hardship or concession data, should only be transferred at express specific election of the Consumer Data Right consumer and/or once the offer of the specific product or service has been accepted;

v. require an Accredited Person to explain why more than a one-off consent to transfer Consumer Data Right Data is required;

vi. mandating what Personal Information of the Consumer Data Right Consumer (if any) needs to be disclosed by the Accredited Person to the Gateway;

vii. enabling the Gateway to refuse to authenticate an Accredited Person because of a belief of harm or misuse to a Consumer Data Right participant or the Consumer Data Right infrastructure;

viii. if Alternative Authentication Model #2 is preferred, the Data Holder should only be required to supplement the data that the Gateway has received from the Accredited Person for the purpose of contacting the Consumer Data Right Consumer for the authentication process. In addition, it should mandate what Personal Information (if any) of the Consumer Data Right Consumer needs to be disclosed by the Data Holder to the Gateway for the purpose of authenticating them;

ix. if authentication is outsourced to a third party, rules which ensure that disclosure of Personal Information during the authentication process is managed via a an appropriate outsourcing arrangement;

x. the Accredited Person must be required to provide any information that is necessary to ensure that the Gateway and Data Holder can appropriately source the Consumer Data Right Consumer's data;

xi. ensuring that the Personal Information of third parties (such as installers) is not shared when a Consumer Data Right Consumer's DER Data is shared; and

xii. depending on the outcome of the consultation into the inclusion of intermediaries in the Consumer Data Right regime, appropriate rules to regulate their conduct in the energy Consumer Data Right.

We also recommend that the ACCC and the DSB review whether or not individuals who are under 18 years of age should be permitted to access the energy Consumer Data Right, and whether access to closed or inactive accounts should be enabled, given the feedback provided by stakeholders and the need to widen the operation of the energy Consumer Data Right for the benefit of electricity consumers.

Agency response: Support in part

Recommendation 3, 3i: Support

The ACCC is considering the issue of eligible consumers in energy Consumer Data Right and will consult on eligible consumer requirements for the energy sector in the energy rules framework. The energy rules framework will seek stakeholder submissions on, among other matters, whether individuals who are under 18 years of age should be permitted to access the energy Consumer Data Right and whether there are compelling use cases for the sharing of retailer-held consumer data sets for inactive accounts. Additionally, the ACCC will seek views on the extent to which persons who have been nominated to transact on the account by the account holder (known as 'authorised representatives' under national energy legislation) should be included as eligible consumers.

Recommendations 3ii, 3vi and 3x: Support

The energy rules framework document will consider the recommendations that relate to data flows of information, including personal information, or notification involving accredited persons and the gateway. The ACCC will continue to engage with stakeholders on these matters through the energy rules framework and other avenues, to reach appropriate privacy outcomes.

Recommendation 3iii: Support

The ACCC is considering, and will seek stakeholder feedback during the development of the energy rules framework document on what adaptations to protections under the current subrule 4.12 are required for the energy sector.

Recommendation 3iv: Support

The ACCC notes that energy Consumer Data Right data sets may encompass potentially sensitive information, such as customer eligibility for concessions, or whether the customer is in a hardship program. While the potential for such data to be shared via the Consumer Data Right is a privacy risk and may cause concern for consumers, there are also arguments in favour of the benefit of consumers being able to seek third party assistance in relation to the data. This issue will be explored through consultative rules development. As a first step the energy rules framework consultation will seek stakeholder views on whether any particular sensitive information should be explicitly excluded from customer data or, if not excluded, unclustered from other data to allow Consumer Data Right Consumers additional control over whether the information is shared.

Recommendation 3v: Support

Rules related to Energy will be made in a manner that complements existing Consumer Data Right rules to reduce duplication and ensure consistency within the Consumer Data Right. Consumer Data Right Rule 4.11(3)c) requires accredited persons, when seeking consent from a Consumer Data Right consumer, to provide information about how the accredited person is complying with the data minimisation principle. This includes explaining how the collection of Consumer Data Right data is reasonably needed, and relates to no longer a time period than is reasonably needed. Further, Rule 4.11(1)(b) of the Consumer Data Right rules specifies that the Consumer Data Right consumer must be enabled to actively select or otherwise clearly indicate the period over which Consumer Data Right data will be collected and used.

The ACCC therefore considers that the Consumer Data Right rules currently implement this recommendation, and the ACCC expects to maintain these requirements for the energy Consumer

Data Right rules, subject to ensuring that consumers are not presented with excessive information in consent screens.

Recommendations 3vii: Support

The ACCC will consider the role of the AEMO as Gateway in respect of verifying accredited persons. Where appropriate this may include enabling the AEMO to refuse to authenticate an accredited person. We note that similar enabling provisions are provided for data holders in relation to the current version of the Rules. We intend to consult in the Consumer Data Right energy rules framework document on the circumstances in which AEMO should have this ability.

Recommendations 3viii and 3ix: Support

The ACCC is examining the appropriate authentication model for energy Consumer Data Right. The ACCC intends to consult on two authentication models in the energy rules framework document. As outlined in the response below to Recommendation 4, the level of privacy risks associated with the two authentication models is an important consideration. Consistent with the requirements of the Act in relation to gateways and the approach to Consumer Data Right rulemaking in relation to personal data, it is contemplated that the use of data by gateways will be tightly controlled and that strong information security arrangements will be required. Finally, if the ACCC considers it may be appropriate to permit a Consumer Data Right participant to outsource part or all of its authentication obligations to a third party, we will consider the development of rules to ensure that personal data is appropriately managed as part of any such outsourcing arrangement.

Recommendation 3xi: Support

The ACCC is examining the issue of preventing the sharing of Personal information of third parties in Distributed Energy Resource (DER) Data. The ACCC will consult on the delineation of datasets, including DER data, in the energy rules framework document. It is important that appropriate protections be in place to limit the risk of sharing Personal Information about third party individuals in DER data.

Recommendation 3xii: Support

Contingent on the outcome of the ACCC consultation commenced on 23 December 2019 on facilitating participation of intermediaries in the Consumer Data Right regime, appropriate rules may be developed to regulate intermediaries' conduct in the Consumer Data Right regime as a whole.

Further response:

While the recommendation is directed at the contents of the Rules, it should be noted that the data standards will also play a key role in ensuring that the design of the regime appropriately ensures that privacy concerns are addressed in relation to the above issues.

The Data Standards Chair (Chair) is responsible for making and reviewing Data Standards about the format and description; disclosure; collection, use, accuracy, storage, security and deletion; and de-identification of Consumer Data Right data. The objective, and value, of the Standards is in enabling consistent technical interfaces that allow for the safe, efficient and convenient transfer of consumer data. In order to meet this objective, the Chair, amongst other things, actively seeks advice on information security, privacy and consumer behaviour matters. The Consumer Data Right is intended to flow across all sectors of the economy, however, the Chair is mindful of the sensitivity of the data from each sector, as well as relevant sectoral issues for the consumers.

From the beginning of the Consumer Data Right the Chair, assisted by the DSB, has undertaken a highly transparent consultation approach for a public sector Standards development process, which was designed to be open and available to anyone who is interested. This stakeholder engagement model has included the use of different channels designed to engage various communities, such as a public Github portal, in-person and now virtual workshops, email updates, blogs and working groups. Several Electricity sector specific workshops were held in the first half of 2020. These channels allow for robust

exchanges of opinions, with critiques and suggestions informing the direction of the Standards, and initiating change.

The Chair has also been advised by a well-represented Data Standards Advisory Committee (DSAC), and since 2019, a dedicated Energy Data Standards Advisory Committee (EDSAC). The DSAC and EDSAC both include Consumer and Privacy Advocates, as well as industry representatives.

The DSB also conducts Consumer Experience (CX) research in order to provide CX Guidelines and CX Standards for the Australian context. This CX research also provides insights and evidence that informs policy and Rule formation. The extensive research undertaken includes industry consultation, and in collaboration with various government agencies, as well as behavioural and consumer research with a diverse range of individuals from across the Australian public. In order to strengthen this research, the DSB has commenced a collaboration with the Consumer Policy Research Centre (CPRC) in order to support community sector and consumer advocate consultation. At the time of writing, the CPRC has commenced a review of the CX Standards and Guidelines in order to assess, among other things, how well they cater to existing consumer needs and expectations, including people experiencing vulnerability.

KPMG recommendation 4 – Authentication model

The ACCC has proposed two alternative authentication models described in Part 8 of this report. The ACCC will need to consider the risks and our observations in this report when determining which authentication model to use. Both have advantages and disadvantages that need to be weighed against the privacy impacts of each model. Based on our analysis, it appears that Alternative Authentication Model #1 has comparatively fewer privacy risks, despite the barrier of less sophisticated Electricity Retailers having to develop their own authentication processes. Since most Electricity Retailers have digital platforms to connect with their customers, we do not believe that this disadvantage is detrimental to this authentication model in the long term.

We recommend the ACCC consider Alternative Authentication Model #1 for authentication purposes given it has comparatively fewer data flows, avoids the Gateway receiving additional data that it could associate with a National Metering Identification number (NMI) and ensures the Electricity Retailer develops a robust system to authenticate the Consumer Data Right Consumer prior to seeking their authorisation.

Agency response: Support in principle

The ACCC intends to consult on the two alternative consumer authentication models described by Part 8 of this report in order to make an informed and appropriate decision regarding authentication for the gateway data access model in energy Consumer Data Right.

The level of privacy risks associated with each of the two authentication models is an important consideration in making a decision regarding the most appropriate authentication model for energy Consumer Data Right.

We note the recommendation of this SPIA in favour of Model #1 and will take this into account in our future consideration of this issue.

KPMG recommendation 5 – Data access regimes

The current regulatory frameworks applying to the energy sector include the National Customer Energy Framework (NECF) and the Victorian Energy Retail Rules (VERC). Both of these frameworks will continue to operate simultaneously with the energy Consumer Data Right. The relevant regulatory bodies including the Australian Energy Market Commission (AEMC), the Australian Energy Regulator (AER), and Essential Services Commission (ESC) will need to consider how both regimes will operate to enable Electricity Retailers to operate in a compliant manner with the Consumer Data Right. We recommend that Treasury and the ACCC engage with these bodies and the Council of Australian Governments (COAG) Energy Council to consider and assess the impact of the energy Consumer Data Right on the existing data access regimes.

Agency Response: Support

The ACCC and Treasury will continue to engage with stakeholders including the AEMC, AER, ESC and the COAG Energy Council to ensure that the impacts of energy Consumer Data Right on existing data access regimes are managed appropriately.

While it is desirable that industry participants are not unduly subject to multiple data access requirements, there are differences in the functionality and purpose of different requirements. In particular, some energy sector specific requirements are directed at human readable data provision in particular formats – while the Consumer Data Right is primarily directed at machine readable data access and where human readable access for consumers is required, this is not subject to specific formatting obligations. However, direct to consumer sharing is not envisaged in the first version of the energy Consumer Data Right.

The COAG Energy Council is working to amend the energy regulatory framework to facilitate the operation of the Consumer Data Right for energy. These changes are intended to ensure that the energy regulatory regime does not act as a barrier to the operation of the Consumer Data Right for energy in regards to data that is collected and handled under energy law.

The energy regulatory framework will continue to provide a way for consumers to access their metering data directly from their retailer and distributor, with the Consumer Data Right providing an option to share data with third parties.

KPMG recommendation 6 – Data quality

The current sources of data used by the energy sector contain inherent issues in relation to the format and quality of data, which is an issue known and identified by stakeholders. We understand that these systemic issues require a substantial time and cost investment to address, and the Consumer Data Right may amplify some of these issues from a privacy perspective. We recommend that Treasury work with participants from the energy sector to understand what additional improvements can be made to the current systems they use to limit the risk of Personal Information being shared with a Consumer Data Right Consumer that is not theirs and to ensure consistency.

Agency Response: Support in principle

Privacy Safeguard 11 – quality of Consumer Data Right data (s56EN of the Act) provides in part that "… [i]f a data holder of Consumer Data Right data is required or authorised under the consumer data rules to disclose the Consumer Data Right data, the data holder must take reasonable steps to ensure that the Consumer Data Right data is, having regard to the purpose for which it is held, accurate, up to date and complete…".

This is supplemented by a number of provisions empowering the ACCC to make rules regarding the accuracy of Consumer Data Right data (e.g. ss56BB, 56BC, 56BE and 56BG of the Act), obligations to correct inaccuracies (Privacy safeguard 13—correction of Consumer Data Right data (s56EP)) and to notify persons of corrections (s.56EN(3) and (4) of the Act).

Development of rules regarding accuracy of data will form part of the proposed rulemaking process for the Consumer Data Right for Energy. The need to limit the risks arising in relation to the format and quality of data will be examined, in consultation with energy sector stakeholders, to determine if any specific requirements are required in the energy sector to address this privacy risk.

Working with industry participants to ensure awareness and compliance with the data accuracy obligations provided for in the Privacy Safeguards and any supporting rules will form part of the industry education and compliance work of Consumer Data Right agencies.

Ensuring data is provided in consistent and appropriate formats will occur largely through Consumer Data Right standards setting processes. The Data Standards Body is responsible for the setting of standards for the format of data payloads to ensure consistency and interoperability. The DSB is obliged by the Consumer Data Right Rules to engage in consultative data setting processes.

KPMG recommendation 7 – Priority Energy Datasets

Noting that the Priority Energy Datasets are intended to be broadly defined in the Designation Instrument, we recommend that it identifies as clearly as possible what data types (or classes) are in scope and what are out of scope, and that the Consumer Data Standards explain what types of data will be included with the scope of each of the datasets identified in the Designation Instrument. This will enable the Data Holder and the Gateway to reconfigure or adjust their databases so that they can respond accurately and in a timely manner to a Consumer Data Request. This will also help avoid data not aligned to the Consumer Data Standards being disclosed by the Data Holder or the Gateway that contains data that the Consumer Data Right Consumer did not consent to be transferred.

Agency Response: Support

The draft designation instrument was released for public consultation from 6 May 2020 to 31 May 2020. Submissions were received from nineteen stakeholders, with two submitted in confidence.

The draft instrument seeks to identify clearly, which data sets and data holders are within the scope of the ACCC's Consumer Data Right rulemaking power.

It should be noted that the data sets subject to the Consumer Data Right will be further refined through the ACCC rulemaking and Data Standards Body standard setting. Through these rulemaking and standard setting processes, particular inclusions and exclusions will be identified, consulted upon and specified. A further Privacy Impact Assessment will be undertaken before the rules are made. All rules, including those relating to dataset coverage, require Ministerial consent and are subject to Parliamentary disallowance.

Ultimately, the exact datasets that must be provided in response to consumer authorised requests will be set out in detail in data payload standards made by the Data Standards Body. The process for establishing the specifics of these payloads, and the development of the language by which consumers understand them (referred to as 'data clusters') are undertaken through the Standards development processes and the CX research workstream respectively, as outlined in the response to recommendation 3.

The standards will inform the information technology builds of Consumer Data Right participants and, by operation of the Privacy Safeguards and the ACCC rules, some will be enforceable by the OAIC and ACCC. Standards are also enforceable between Consumer Data Right participants as a multilateral contract.

KPMG recommendation 8 – Conduct of other PIAs

We recommend that a separate PIA should be considered for the following components of the energy Consumer Data Right if they are proposed to be introduced:

- the inclusion of third party authentication service providers in the energy Consumer Data Right;
- a tiered accreditation model for ADRs;
- the inclusion of other energy datasets including value-add or enhanced datasets, circuit-level metering, data from sub-meters and data obtained from managed home devices (noting these may be collected and used outside of the Consumer Data Right environment);
- extension of the energy Consumer Data Right, including the application to gas services; and
- the rights of energy Consumer Data Right consumers to access their data directly.

Agency Response: Support

See our response to **Recommendation 1**.

A supplementary PIA is proposed to be conducted that will cover all of the identified issues that relate to rulemaking (e.g. tiered accreditation) or possible future amendments to the sectoral designation (e.g. application of Consumer Data Right to gas metering data).