Consumer Data Right in the Energy Sector

SUPPLEMENTARY PRIVACY IMPACT ASSESSMENT FOR THE COMMONWEALTH DEPARTMENT OF TREASURY

ANALYSIS AS AT 27 APRIL 2020

REPORT FINALISED ON 25 MAY 2020

KPMG AUSTRALIA

NOTICE TO THIRD PARTIES

This report is solely for the purpose set out in **Part 1** and **Part 5** of this report and for the Commonwealth Department of Treasury's information, and is not to be used for any purpose not contemplated in the engagement contract with the Commonwealth Department of Treasury or to be distributed to any third party without KPMG's prior written consent. This report has been prepared at the request of the Commonwealth Department of Treasury in accordance with the terms of KPMG's applicable engagement contract. Other than our responsibility to the Commonwealth Department of Treasury, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility. The information contained in this report is of a general nature and is not intended to address the specific circumstances of any particular individual or entity. Appropriate professional advice should be obtained before acting on this information.

The views and opinions expressed herein are those of the author and do not necessarily represent the views and opinions of KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International.

KPMG

Contents

KPMG

Part 1. Introduction and Structure of this Report

1.1 Overview and context

a. KPMG[1] is very pleased to provide this supplementary privacy impact assessment report (**report**) to the Commonwealth Department of the Treasury (**Treasury**).

b. This report has been prepared as a result of an independent supplementary privacy impact assessment (**SPIA**) that has been conducted by KPMG in relation to the proposed designation of the National Electricity Market (**NEM**) to which the Consumer Data Right regime (**CDR**) will apply. The NEM does not include Western Australia and the Northern Territory, and for the purposes of this report will be referred to as **the energy sector**. This assessment follows consultation by Treasury on the extension of the CDR to the energy sector and proposed designation of Priority Energy Datasets, to enable the Australian Competition and Consumer Commission (**ACCC**) to develop rules governing how the CDR will operate in the energy sector.

c. The CDR was introduced by the Commonwealth Government in August 2019.[2] The banking sector was the first sector of the Australian economy in which the CDR has been introduced following its designation (**Open Banking**).[3] This report follows from and supplements the extensive independent privacy impact assessments and analyses undertaken for Treasury in relation to the establishment of the CDR and Open Banking, which was completed at the end of 2019. Since then, the legislative framework that underpins and forms part of the CDR has been progressed, specifically the CDR Rules have been finalised and implemented and the Consumer Data Standards, Consumer Experience (**CX**) Standards and the CDR Privacy Safeguard Guidelines have been published. This legislative framework continues to evolve as the CDR is introduced in Open Banking in a phased approach and the designation of the energy sector is now being further considered.

d. In conducting this SPIA and preparing this report, KPMG appreciates the opportunity to contribute to the progression of this important Australian data right regime and the benefits it will deliver to consumers across the economy. Ensuring that appropriate consideration is given to the particular privacy impacts of designating the energy CDR after Open Banking, and putting in place further appropriate privacy protections or mitigations to protect consumers from unnecessary harms that are as far as possible consistent with the current CDR framework, will support this objective.

e. It is important to note that this report reflects an analysis of the privacy risks at a 'point in time' in the development of the energy CDR, prior to the publication by Treasury of the exposure draft of the Designation Instrument for energy and at a time when stakeholders are continuing to assess the impact of and prepare for the designation and implementation of the energy CDR.

f. KPMG acknowledges the valuable contribution from stakeholders and the time they have taken to share their current views within a short timeframe, which is very much appreciated. Their responses and collaborative feedback has helped us to prepare this SPIA and has contributed to further the understanding of the privacy impacts and safeguards required for implementing the energy CDR.

[1] Which includes KPMG Law.
[2] The CDR was enacted by the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) to insert Part IVD into the CCA.
[3] *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (Cth), 4 September 2019.

1.2 Executive summary

a. This report has been prepared having regard to:

   i. the objectives of the energy CDR and the features of the energy CDR for a minimum viable product;

   ii. key information reviewed by KPMG as at 27 April 2020 (described further in **Appendix 3** to this report);

   iii. views expressed by stakeholders that we consulted listed in **Appendix 4** to this report;

   iv. information shared by Treasury and the ACCC in relation to the current proposed authentication models for the energy CDR;[4] and

   v. the privacy impact assessment conducted for the implementation of the CDR in banking which was the subject of a finalised report dated 29 November 2019 (**CDR PIA**).[5]

b. A PIA is a detailed analysis of particular Personal Information flows and potential privacy risks and impacts (both negative and positive) from a proposed project at a point in time. It may be reviewed and updated at particular times in the future to reflect the impact of any changes or updates to the project, having regard to the nature of the project, risks and recommendations. This can help to understand if the risks have changed, whether new risks have emerged, if the recommendations remain appropriate or have been implemented, and, if so, what effect they have had.

c. The purpose of this SPIA for the energy CDR at this point in time is to assess the additional privacy impacts and risks from the proposed designation beyond the status quo of what energy consumers can currently access under the current National Energy Customer Framework (**NECF**) (and the Victorian Energy Retailer Code (**VERC**)) which apply to the energy sector. This SPIA has had regard to, in particular:

   i. the current regulatory framework in the energy sector as summarised in this report;

   ii. the proposed Priority Energy Datasets that will be included in the Designation Instrument and the data flows, noting energy consumers will not be given direct access to their CDR data at this stage;

   iii. the gateway(s) that are proposed to be designated and the proposed participants in the energy CDR;

   iv. proposed consumer authentication, consent and authorisation processes for the energy CDR;

   v. data disclosure and collection, use, accuracy and integrity, storage, security, deletion and de-identification of proposed Priority Energy Datasets; and

   vi. consumer rights (including complaints handling and exercise of rights).

[4] It should be noted that the information that was shared by Treasury and the ACCC was provided to assist our understanding of the current policy approach for the energy CDR at the time of conducting this SPIA and preparing this report. Any particular views that may be inferred from this report should not be taken as views that are endorsed by Treasury, the ACCC, or the Commonwealth Government.
[5] An initial PIA was conducted internally by Treasury (with external assistance) and published by Treasury on 1 March 2019. Treasury responded to the CDR PIA on 11 December 2019.

1.3 Structure of this report

a. The structure of this report is set out as follows:

i. **Part 2 (Summary of Findings and Recommendations)** explains our findings and recommendations based on our scope of and approach to this SPIA;

ii. **Part 3 (Background)** provides an overview of Treasury's and the ACCC's approach to date in relation to the designation of the energy CDR, and important developments to the CDR regime since the publication of the CDR PIA;

iii. **Part 4 (Objective of this SPIA)** describes the supplementary nature of this SPIA and how it will present different or additional risks to those identified in the CDR PIA (which focused on Open Banking) given the focus of this SPIA is on the energy CDR;

iv. **Part 5 (Scope and Assumptions of this SPIA)** explains why this SPIA is a point-in-time assessment and the assumptions that have been made to provide clarity to readers about the breadth and depth of our considerations;

v. **Part 6 (Methodology)** summarises our approach to conducting this SPIA and outlines the publicly available information that we reviewed, the stakeholders that we consulted and any information that we received from Treasury and the ACCC to guide our thinking on currently policy deliberations;

vi. **Part 7 (Energy CDR and its Key Features)** describes the focus of the designation of the energy CDR. Following a discussion about the energy sector structure and its regulatory frameworks, we explore participants in the energy sector and the applicable privacy regulatory framework that applies to the participants. This then leads to a discussion about the Priority Energy Datasets, and the key features and privacy considerations for data access in the energy sector. To provide further context prior to Part 8 of this report, key concepts for the energy CDR and the energy CDR data flows are canvassed;

vii. **Part 8 (Analysis of Privacy Impacts and Risks)** analyses the privacy impacts and risks from the data flows based on two proposed authentication models. Risks are identified, together with existing mitigation strategies and suggested recommendations based on a gap analysis; and

viii. **Part 9 (Other Privacy Risks, Issues and Considerations)** explores other privacy risks, issues and considerations that we identified, based on our consultations with stakeholders and review of information and materials supplied to us, and that we have included in this report because of their relevance to the impact of the development of the energy CDR.

Part 2. Summary of Findings and Recommendations

2.1 Summary of findings

a. This section includes a summary of the key privacy impacts and risks that we have identified from the designation of the CDR in the energy sector. It is followed by a summary of key recommendations that we have made as a result of our analysis of the risks and impact, having regard to the scope and assumptions detailed in **Part 5** of this report and following our methodology described in **Part 6** of this report. We have also considered the responses from Treasury and the ACCC following the submission of our draft SPIA dated 27 April 2020.

b. The risks that we have identified relate to the energy CDR at this point in time. These privacy risks supplement the risks identified in the CDR PIA and are not intended to repeat the findings raised in the CDR PIA. We note that some of the risks that we have identified may amplify the risks that currently exist in the energy sector. We describe the existing features and data access framework for the energy sector in **Part 7** of this report and note that the energy CDR develops greater rigour around particular data transfer and access processes.

c. These key privacy risks are:

   i. **Risk 1** – the CDR framework is complex and it creates additional compliance requirements that the energy CDR participants (including Gateways) will need to meet.[6] These requirements are in addition to the existing requirements in the regulatory framework that apply to the energy sector under NECF and the VERC and the Privacy Act. These additional requirements on the CDR participants in the energy sector may result in confusion about, or inconsistency in complying with, their obligations and rights, including when CDR Data that they process is governed by an energy sector regulatory requirement, a rule under the CDR Rules, an APP and / or a CDR Privacy Safeguard having regard to their role as a particular type of CDR participant;

   ii. **Risk 2** – the different approaches and policies that Electricity Retailers as Data Holders have to manage in relation to their customer's electricity accounts and data access procedures within the current energy regulatory framework which are more focussed on an individual accessing their own data. An Electricity Retailer may allow an account to be jointly held by more than one individual and a primary account holder may authorise others to access and use the account in particular ways. This means that in addition to the primary account holder who could be a CDR Consumer for an account, the rights and obligations of other individuals who are associates of or who deal with the CDR Consumer will be impacted and the extent to which they can be an Eligible CDR Consumer needs to be considered;

   iii. **Risk 3** – the introduction of the AEMO Gateway Model through which the Priority Energy Datasets will flow, will involve the sharing of CDR Data through a new entity, the Australian Energy Market Operator (**AEMO**) who:

      1. will be both a Data Holder (for particular Priority Energy Datasets) and a Gateway;
      2. does not currently have a direct consumer-facing role;
      3. will need to be involved in the authentication process to be applied to an Eligible CDR Consumer, whether directly or indirectly;
      4. will transmit CDR Data from one or more Data Holders to Accredited Persons through its platform and systems; and
      5. will disclose CDR Data in its capacity as a Data Holder.

      The ACCC's view of the AEMO as the preferred gateway under the AEMO Gateway Model was based on a number of privacy-related factors, having regard to its role and the data it collects and transmits, which relevantly included ensuring the security and privacy of the data, user functionality and interoperability. In addition to these factors, a number of other factors were also considered, including existing technological infrastructure and systems, cost effectiveness and flexibility.

      Should the AEMO have a data breach, this will expose the CDR Data to further security risks. There is also currently a lack of understanding from stakeholders as to how the Priority Energy Datasets, for which the AEMO will not be a Data Holder, will be transmitted by the Gateway. This means that there are potential privacy risks that need to be addressed should the AEMO collect, access or use these datasets. The CDR Rules commenced and the CDR Privacy Safeguard Guidelines were published at a time when there were no designated gateways for Open Banking.

[6] Any reference to 'CDR participant' in this report includes a Data Holder, Accredited Person / ADR, and Gateway.

The authentication processes and data flows for a Gateway in the energy sector have not yet been finalised;

iv. **Risk 4** – the nature of the Priority Energy Datasets and how they are defined and applied in the energy sector, including their format and perceived sensitivity. Unless the scope of the Priority Energy Datasets are clearly defined and the specific data types to be included are made clear and will be subject to specific consents, Data Holders may disclose more information than the CDR Consumer expected. That may include information that the CDR Consumer considers sensitive and did not want to be disclosed.

In particular, Metering Data from the Priority Energy Datasets reflects the aggregate consumption of electricity that passes through a meter (or meters) that has a prescribed NMI. The data does not reflect the consumption of electricity by a particular individual, unless that individual is the sole occupant of and user of energy at the property to which the NMI is attributed. In the majority of scenarios, multiple occupants reside at a premises. This means that the usage information of third parties could be included in CDR Data that is disclosed to Accredited Persons without their knowledge and consent. It also raises the question of how they could be adequately identified as an Eligible CDR Consumer to participate in the energy CDR in connection with data that relates to them;

v. **Risk 5** – the current status of stakeholders' limited understanding of the AEMO Gateway Model and how it will operate to transmit the Priority Energy Datasets from Data Holders to Accredited Persons. While a preference for the design of the data access model has been shared, stakeholders expressed that they do not currently have a comprehensive understanding of how the AEMO will transmit the CDR Data from the Data Holder to the Accredited Person and to what extent and on what basis it may need to otherwise access and process the CDR Data it is transmitting;

vi. **Risk 6** – the existing risks that are inherent in the energy sector (e.g. data quality and integrity issues) are amplified by the transfer of the Priority Energy Datasets through the Gateway and to additional third parties (i.e. Accredited Persons). Personal Information is also routinely disclosed to incoming Electricity Retailers where account holders shift to a new Electricity Retailer. This involves risks relating to inaccuracies in the data being shared, errors in authenticating the consumer and the issues of account holders, authorised representatives and other occupants;

vii. **Risk 7** – the current CDR Rules exclude individuals under 18 years of age accessing the CDR and do not include closed or inactive accounts. Individuals under 18 years of age, and individuals wishing to access data from a closed or inactive account, cannot currently be classified as an Eligible CDR Consumer. Some individuals under 18 years of age contract with Electricity Retailers for electricity services but many do not. The data about their energy consumption and from a closed or inactive account, may assist an ADR with its good or service offering. However, there are currently no rules to address these scenarios; and

viii. **Risk 8** – the CDR Consumer will be the account holder and may be the owner of the property. If the owner sells or transfers the property to another individual, the CDR Consumer may continue to receive goods or services from the ADR who is continuing to collect CDR Data. Following the sale or transfer, the CDR Data will be about another person. If the Data Holder does not notify the Accredited Person or the Gateway of this change in circumstances, data about another individual may be disclosed to a third party without consent.

d. Each risk is analysed and discussed in more detail in **Part 8** of this report. The analysis takes into account the privacy protections that have been built into the CDR legislative framework to date (as further detailed in the CDR Rules, and supported by the Consumer Data Standards, CX Standards and CDR Privacy Safeguard Guidelines), which reflect some of the recommendations in the CDR PIA. The recommendations we have made are intended to mitigate or further mitigate the identified risks, having regard to their likelihood or seriousness, as well as the proposed designation of the energy sector and the future development of any

energy-specific CDR Rules, Consumer Data Standards, CX Standards and CDR Privacy Safeguard Guidelines.

2.2 Summary of recommendations

We have made recommendations in this report which are summarised below (and should be read together with the more detailed and relevant parts of this report):

a. **Recommendation 1**: **Further updates to this SPIA** *[responsibility: Treasury with the assistance of the ACCC]*

Our assessment and analysis has been undertaken at a point in time in relation to the development of the CDR, the phased introduction of Open Banking and the proposed designation of CDR in the energy sector. Noting that this 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 CDR 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.

b. **Recommendation 2**: **The Gateway** *[responsibility: the AEMO, Treasury, DSB, ACCC and OAIC]*

We **recommend** that a PIA be conducted on the proposed platform and systems that may be used for the Gateway with the involvement of AEMO, Treasury, the ACCC, the OAIC and the 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 CCA, 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 CDR 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 CDR Privacy Safeguards and APPs will interact and apply to the Gateway in light of its role and the CDR Data that it transmits / flows through it and which it collects and holds.

c. **Recommendation 3: Matters for the energy rules to address** *[responsibility: ACCC, OAIC and DSB]*

Having regard to the objective of a consistent and interoperable CDR framework, the energy-specific CDR 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 CDR Privacy Safeguard Guidelines, Consumer Data Standards, CX Standards and CX Guidelines.

We **recommend** that, to the extent not already addressed by the CDR Rules, the energy-specific CDR 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 CDR Consumer is no longer an Eligible CDR Consumer, and when the CDR Consumer became an Eligible CDR Consumer;
iii. review of CDR 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 CDR 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 datasets that would be considered to be more sensitive, such as Hardship or concession data, should only be transferred with the express and specific election of the CDR 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 CDR Data is required;
vi. mandating what Personal Information of the CDR 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 CDR participant or the CDR infrastructure;
viii. if Alternative Authentication Model #2 is preferred,[7] 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 CDR Consumer for the authentication process. In addition, it should mandate what Personal Information (if any) of the CDR 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 are developed to ensure that the disclosure of Personal Information during the authentication process is managed via 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 CDR Consumer's data;
xi. ensuring that the Personal Information of third parties (such as installers) is not shared when a CDR Consumer's DER Data is shared; and
xii. depending on the outcome of the consultation into the inclusion of intermediaries in the CDR regime, appropriate rules to regulate their conduct in the energy CDR.

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 CDR, 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 CDR for the benefit of electricity consumers.

d. **Recommendation 4: Authentication model** *[responsibility: Treasury and ACCC]*

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

[7] See **Part 8** of this report for a description of Alternative Authentication Model #2.

with a NMI and ensures the Electricity Retailer develops a robust system to authenticate the CDR Consumer prior to seeking their authorisation.

e. **Recommendation 5: Data access regimes** *[responsibility: Treasury and ACCC]*

The current regulatory frameworks applying to the energy sector include the NECF and the VERC. Both of these frameworks will continue to operate simultaneously with the energy CDR. The relevant regulatory bodies including the AEMC, AER and ESC will need to consider how both regimes will operate to enable Electricity Retailers to operate in a compliant manner with the CDR. We **recommend** that Treasury and the ACCC engage with these bodies and the COAG Energy Council to consider and assess the impact of the energy CDR on the existing data access regimes.

f. **Recommendation 6: Data quality** *[responsibility: Treasury]*

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 to and identified by stakeholders. We understand that these systemic issues require a substantial time and cost investment to address, and the CDR 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 CDR Consumer that is not theirs and to ensure consistency.

g. **Recommendation 7: Priority Energy Datasets** *[responsibility: Treasury and DSB]*

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 classes of information are in scope and what are out of scope, and that the Consumer Data Standards explain what types of data will be included within the scope of each class of information 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 CDR Consumer did not consent to be transferred.

h. **Recommendation 8: Conduct of other PIAs** *[responsibility: ACCC with the assistance of Treasury]*

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

i. the inclusion of third party authentication service providers in the energy CDR;
ii. a tiered accreditation model for ADRs;
iii. 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 CDR environment);
iv. extension of the energy CDR, including the application to gas services; and
v. the rights of energy CDR Consumers to access their data directly.

Part 3. Background

3.1 Overview

a. Since early 2019, Treasury and the ACCC have conducted public consultations on how best to apply the CDR in the energy sector. Consultations to date have enquired about the designation of Priority Energy Datasets and the data access model, including the type of energy sector participant. In addition, Data61, in its role as the Data Standards Body (**DSB**), has been consulting on the technical data standards and CX standards that will underpin the data access regime to ensure a practical and beneficial consumer experience.

b. One of the main features of the energy CDR that has been considered to date is that the AEMO will act as the Gateway for the transfer of energy CDR Data between energy Data Holders and Accredited Persons / Accredited Data recipients (**ADRs**).[8] The ACCC's criteria for selecting the preferred gateway model included security and privacy, user functionality, cost of infrastructure, scalability and interoperability. Once Treasury has published an exposure draft of the Designation Instrument for the energy sector (and this is approved by the Commonwealth Government), the ACCC has the power to make rules, in consultation with the OAIC and the DSB, that will determine how the CDR functions in the designated sector. The ACCC plans to release an 'Energy Rules Framework' in June 2020 for consultation (following the release of a draft Designation Instrument). This will outline the main features of the energy CDR and form the basis for energy-specific CDR rules.

c. Treasury has the power under sub-section 56AD(2) of the *Competition and Consumer Act 2010* (**CCA**) to implement a Designation Instrument for the CDR in a particular sector of the Australian economy. Before designating the energy sector, the Minister must, under section 56AD of the CCA, consider the likely effect of making the instrument with respect to the interests of the consumer and the privacy or confidentiality of their information. To assist the Minister in making a decision, KPMG was engaged by Treasury on 23 March 2020 to conduct a SPIA on the designation of the energy CDR that will help the Minister understand the privacy impacts (both positive and negative) of the energy CDR.[9]

3.2 CDR regime developments

a. The CDR PIA identified privacy risks and appropriate mitigation strategies in relation to Open Banking based on available information at a particular point in time (i.e. analysis as at 23 September 2019). Since the CDR PIA, the following important developments to the CDR have occurred that are relevant to this SPIA:

   i. **Gateway access model**: on 25 February 2019, the ACCC sought stakeholder views on three data access models for energy data in the energy sector, and the relevant principles and considerations for assessing data under these models. The consultation on these proposed data access models concluded on 22 March 2019. On 29 August 2019, the ACCC published a position paper setting out the AEMO Gateway Model as the ACCC's preferred data access model for the CDR regime in the energy sector.[10] In this position paper, the ACCC noted that the data access model impacts the authorisation and authentication arrangements for the energy sector, the standards that will be developed and the allocation of liability;

   ii. **Priority Energy Datasets**: between 29 August 2019 and 26 September 2019, Treasury held a consultation on the priority energy CDR datasets.[11] Treasury sought stakeholder views on the

[8] We note that *Energy made Easy* (managed by the AER) and *Victorian Energy Compare* (managed by the DELWP) may also be designated as Gateways for PRD.
[9] A draft of this report was submitted to Treasury on 27 April 2020. This SPIA may also satisfy the requirements under the *Australian Government Agencies Privacy Code* given the designation of the CDR in the energy sector may be considered a 'high privacy risk' project.
[10] The ACCC's Consumer Data Right in Energy, Position Paper: Data Access Model for Energy Data, August 2019.
[11] Treasury's Priority Energy Datasets Consultation, Consumer Data Right, 29 August 2019.

scope of the energy sector datasets and energy market entities that should be subject to an energy CDR in the Designation Instrument. Following the completion of the consultation, on 9 January 2020 the Government agreed in-principle to the coverage of CDR datasets and Data Holders in the energy sector (described in **Section 7.4** of this report). The consultation did not refer to value-added or materially enhanced datasets;

iii. **External Dispute Resolution**: Treasury has been leading work on an external dispute resolution scheme for the CDR beyond Open Banking and has consulted the various State energy Ombudsmen, with whom KPMG has also consulted. Internal dispute resolution arrangements are likely to be similar to Open Banking, but adopting specific arrangements relevant in the energy sector;

iv. **Intermediaries**: on 23 December 2019, the ACCC released a consultation paper seeking stakeholder views on how the CDR rules should permit the use of third party service providers that collect or facilitate the collection of CDR data from Data Holders on behalf of Accredited Persons (**intermediaries**). The ACCC also sought views on permitting the disclosure of CDR Data from Accredited Persons to non-accredited third parties and the appropriate consumer and privacy protections that should apply to such disclosures. The consultation closed on 3 February 2020, submissions have been published by the ACCC and the ACCC will be publishing its observations in the future;[12]

v. **Commencement of CDR Rules**: the final CDR rules made by the ACCC for the CDR and Open Banking were published by the ACCC and commenced on 6 February 2020 following the consent from the Treasurer of the Commonwealth Government;

vi. **CDR Privacy Safeguard Guidelines**: the OAIC published the *CDR Privacy Safeguard Guidelines* in February 2020 under section 56EQ(1)(a) of the CCA;

vii. **Inquiry into Future Directions for the Consumer Data Right**: in January 2020, the Treasurer of the Commonwealth Government announced an inquiry into the future directions for the CDR and released an Issues Paper in March 2020. The focus of this inquiry is to assess how the CDR can be enhanced or leveraged to boost innovation and competition in the Australian economy, while ensuring that the development of the CDR is safe and secure, efficient, and benefits Australians and the Australian economy;

viii. **Consumer Data Standards**: the DSB has published updated Consumer Data Standards (v 1.3.0), and updated CX Standards and supporting CX Guidelines (v 1.3.0) as at 17 April 2020; and

ix. **Impact of COVID-19**: the novel Coronavirus (**COVID-19**) has impacted various aspects of the Australian economy, including the progression of the CDR. In relation to Open Banking, delays have been experienced in relation to its implementation, and it is likely that COVID-19 will impact the development and implementation of the energy CDR.

b. The DSB has also taken steps to support the development of the energy CDR. With its role in developing the Consumer Data Standards, the DSB established an Energy Data Standards Advisory Committee (**EDSAC**) to invite collaboration on these developments from interested stakeholders. The primary role of the EDSAC is to consider all current and significant issues from both a consumer and industry perspective so that the Consumer Data Standards for the energy sector are drafted to maximise the benefits for consumers. In addition, the DSB released in March 2020 its *Consumer Experience Research (Phase 3: Round 1 and 2) Report* and in April 2020 its *Consumer Experience Research (Phase 3: Round 3) Report* which includes a focus on the energy sector, joint accounts, de-identification and deletion.

[12] The ACCC's Consumer Data Right, Consultation on How Best to Facilitate Participation of Third Party Service Providers, December 2019. The ACCC has not published a notice in relation to the expected time frame for the publication of its position following the consultation.

Part 4. Objective of this SPIA

a. It is only once the energy sector is designated for the CDR by the Treasurer of the Commonwealth Government that the detailed design and specific rules for the energy CDR will be developed by the ACCC. At this point in time, the objective of this SPIA is to provide recommendations to Treasury to mitigate any risks and impacts identified in relation to the privacy of consumers based on the proposed model for the energy CDR as at 27 April 2020 and to assist the ACCC in formulating the proposed approach to the energy CDR rules prior to commencing consultation on the energy rules framework.

b. The aim of an energy CDR is to enable individuals and businesses (both consumers) to have more control over their own data and to give them the right to authorise and direct the secure transfer to, and access in a compliant format of, their energy data by accredited third parties. It would also require the provision of public access to specified energy products. This would allow consumers, for example, to make informed product choices to find and switch to the best energy deals. Over time, this is expected to encourage greater competition between Electricity Retailers and deliver innovative retail products that help consumers better manage their energy use, find better products and make informed decisions about personal energy investments. Other objectives are to ensure that the energy CDR is interoperable with the economy-wide CDR, privacy of consumers' data is protected and CDR participants are held accountable.

c. Privacy impacts can be positive (privacy-enhancing) or negative (privacy-invasive). The objectives of the CDR are aimed at enhancing portability and accessibility of consumers' data to enhance and inform their choice of energy products and services. A privacy risk means that the implementation of the energy CDR will effect a CDR participant's compliance with the applicable privacy obligations, will not meet consumer or community expectations, or not be able to be implemented in a way that does not have unmitigated or unnecessary impacts. There are a range of privacy controls, levers and strategies that may implemented to mitigate or avoid a risk given the nature of the project. Whether some or all of the recommendations described in this report are accepted and implemented by Treasury will have regard to a number of factors and the scope of this SPIA.

d. In this context, the energy CDR will present different or additional risks to those identified in Open Banking that need to be identified and assessed. This assessment is therefore intended to supplement the CDR PIA. Subject to assumptions described in **Part 5** of this report, the focus of this SPIA is on any additional issues and risks not considered or addressed in the CDR PIA or a key difference or change in a particular risk that has been identified and the appropriate mitigation step in the context of:

    i. the proposed Gateway and the current preferred options for authentication, noting that, as Open Banking does not yet include gateways, the CDR PIA did not reference or consider the legislative provisions dealing with designated gateways and privacy risks associated with its potential use;

    ii. the Priority Energy Datasets necessary for a minimum viable product;

    iii. the current CDR Rules, as they would apply to the energy CDR;

    iv. the CDR Privacy Safeguard Guidelines, Consumer Data Standards, CX Standards and CX Guidelines; and

    v. specific matters raised during consultations with stakeholders to date.

e. This SPIA assesses the identified issues and risks against existing and proposed privacy mitigation strategies to manage, minimise or eliminate privacy impacts. This will help influence the Designation Instrument and the development of CDR rules specific to the energy sector so that the regime is well-built to effectively manage privacy risks while having regard to the need to ensure consistency in data access arrangements between sectors as far as possible (at present, between the energy and banking sectors).

Part 5. Scope and Assumptions of this SPIA

This SPIA is based on, and has had regard to, feedback from stakeholders that have been consulted and publicly available information, including information supplied by Treasury and the ACCC that has been authorised for public release.

5.1 Supplementary PIA

This SPIA supplements the CDR PIA. It does not revisit or address certain aspects of the CDR that was the subject of assessment by the CDR PIA. This SPIA does not consider:

a. the data flows between the CDR Consumer and the Accredited Person;

b. the direct data flows between the CDR Consumer and the Data Holder; and

c. the data flows in relation to the ACCC's Register of Accredited Persons and its broader CDR information and communication technology system,

save to the extent these issues are considered in the context of the proposed authentication models and the role of the Gateway as it is currently understood. We note the recommendation made in the CDR PIA in relation to this aspect of the CDR.

5.2 Energy product data

As this SPIA is concerned with the impact on an individual consumer's privacy, to the extent that the Priority Energy Datasets concern Generic Product Data, we have not considered the issues in relation to this dataset in the energy CDR. We have, however, considered the impact of data flowing from the Tailored Product Data dataset.

5.3 Stakeholders consulted

Given the time constraints, the work already undertaken by Treasury and the ACCC, and that this assessment supplements the CDR PIA, KPMG with Treasury and the ACCC identified a number of stakeholders to consult. These stakeholders are listed in **Appendix 4** to this report and include a cross-section of the energy sector based on the information available to date. We did not invite written submissions from the public during the development of this SPIA.

5.4 Point-in-time analysis

a. Like the CDR PIA, this SPIA has been prepared based on the issues and risks assessed at a point in time, noting:

   i. the CDR regime developments described in **Section 3.2** of this report;

   ii. the Designation Instrument for the energy CDR is not yet settled. The draft *Consumer Data Right (Energy Sector) Designation* was released by Treasury on 6 May 2020 for consultation after the analysis for this SPIA concluded on 27 April 2020;

   iii. Open Banking has not yet commenced for public use and is not the subject of this SPIA;

   iv. the final selection of the consumer authentication model for the energy CDR is still under consideration; and

v. that stakeholders are still considering a range of issues relating to the proposed Priority Energy Datasets and the energy CDR framework.

b. The issues raised in this report may be subject to further review and analysis as the design of the energy CDR continues and the details of the data sharing model, consumer authentication process, scope of the Priority Energy Datasets and other relevant arrangements are settled by the ACCC and Treasury.

c. This SPIA has not considered the proposed use of intermediaries who may collect or facilitate the collection of CDR Data from Data Holders on behalf of Accredited Persons (save for in the authentication model analysis) or whether the disclosure of CDR Data from Accredited Persons to non-accredited third parties should be permitted and the appropriate consumer and privacy protections that should apply to such disclosures.

5.5 Current reforms and reviews

We note that the energy sector's regulatory framework (including the review of the NECF to deal with non-traditional energy services and products)[13] as well as the Privacy Act and consumer protections in relation to digital platforms, is currently undergoing review and reform. The Inquiry into Future Directions for the Consumer Data Right is also progressing. The scope of this SPIA does not extend to the examination of the proposed reforms or effectiveness of the current legislation and frameworks. Rather, this SPIA considers the impact of the application of the energy CDR given the current CDR regime and applicable legislative energy and privacy frameworks.

5.6 Other issues and considerations

To the extent that we have identified any issues or concerns of importance that are not related to privacy or personal information in the energy CDR or are not directly within the scope of this SPIA, we have separately noted these at the end of this report.

5.7 Assumptions of this SPIA

a. It is understood that the specific design of the energy CDR is yet to be finalised and policy positions of Treasury and the ACCC are subject to further development and consultation. These include the scope of the energy data to be included in the Priority Energy Datasets, the specific design of the Gateway and the processes to authenticate Eligible CDR Consumers.

b. To support the focus of the assessment on the key issues and the making of reasonably qualified recommendations at a point in time, this SPIA was conducted on the following working assumptions as agreed by the ACCC and Treasury:

i. generally,
   1. we have not considered the issues raised for investigation in the Inquiry into Future Directions for the Consumer Data Right (Issues Paper published March 2020);
   2. we will have regard to publicly available information, views of stakeholders consulted and any information supplied by Treasury and the ACCC (as at 27 April 2020); and
   3. we will consider the privacy impacts of an individual under 18 years of age participating in the CDR;

ii. in relation to the CDR Rules,
   1. we will consider the current CDR Rules "as is" (i.e. we will assume that the CDR environment for the energy sector will involve no intermediaries and there will not be any

[13] See, for example, the AEMC's webpage "How energy consumers are protected under the NECF and ACL", retrieved 4 May 2020.

sharing of energy CDR Data with third parties (other than authorised outsourced service providers of Data Holders and ADRs); and
2. we will not make any observations in relation to whether or not the CDR Rules for the energy sector will align to the National Electricity Rules (**NER**);

iii. in relation to energy consumption or usage data,
1. our review will be based on the Priority Energy Datasets. This does not include data obtained from sub-meters or from home energy management devices;
2. the ACCC intends to consult on including a restriction in the CDR Rules such that Consumer Data Requests will only be made in relation to accounts that are open, not accounts that are closed or inactive at the date of the request. However, there will be no such restriction in the Designation Instrument, and the ACCC's decision is subject to consultation;
3. the data will not be collected in real-time;
4. there will be no direct access by consumers to CDR Data (but consumers mostly have, or can get, access to human readable data outside the CDR regime); and
5. CDR Data will likely be based on a minimum of 12 months' worth of energy consumption to the last date billed, and there will be no minimum period of time in the Designation Instrument or the CDR Rules;

iv. in relation to accreditation,
1. only one tier of accreditation for all ADRs is being considered at this time; and
2. a further PIA in this respect would occur once there is clarity about the introduction of a tiered accreditation system (although the findings of this SPIA regarding issues such as the relative sensitivity of different energy data may be relevant to such considerations);

v. in relation to the AEMO Gateway Model,
1. we will assess the privacy implications in general of the AEMO Gateway Model (and this will not include the AEMO's systems, processes and technology environment);
2. a further PIA would likely occur once the underlying systems and technology used by the AEMO is confirmed; and
3. for Customer Provided Data, Billing Data and Tailored Product Data for which the AEMO is not a Data Holder, the AEMO will only transmit these datasets through to the Accredited Person with the data being held on a transient basis. The CDR Rules cannot authorise the AEMO to access, review or use those datasets (in the data packets) for any purpose other than in accordance with its role as the Gateway;

vi. in relation to the consumer authentication models,
1. the ACCC has shared a working draft of the authentication models for our consideration. These have not been shared with the public, and a consultation and CX testing has not occurred; and
2. we will consider pre-mitigation steps to address identified risks for each option and factors relevant to whether risks can be effectively mitigated; and

vii. in relation to other matters,
1. we will consider the position of joint account holders and authorised representatives in relation to an open account that is the subject of a Consumer Data Request or where these parties may exercise authority in relation to such a request;
2. a meaningful external dispute resolution process will be developed to support the CDR; and
3. we will not focus on any reciprocity principles that will apply to the CDR for the energy sector.[14]

[14] We understand that Electricity Retailers are able to access other types of data beyond the data identified in the Priority Energy Datasets. They may use this data in ways which might make them ADRs, or third party recipients of data outside the CDR regime. We have not considered these issues given the scope of this SPIA.

Part 6. Methodology

a. This SPIA has been conducted in accordance with the OAIC's *Guide to Undertaking Privacy Impact Assessments* (noting that the Privacy Safeguards, rather than the APPs, will generally be the relevant privacy standards in CDR).[15] This SPIA should serve as a living document that supplements the CDR PIA. It does not revisit and reassess all of the risks and issues identified in the CDR PIA, but rather focuses on issues relevant to the proposed designation of the energy CDR in the context of the established CDR framework for Open Banking.

b. This SPIA reflects the findings of the CDR PIA and Treasury's responses, insofar as they apply to the anticipated operation of the energy CDR. The issues and risks in this SPIA have been considered on an 'exception' basis. That is, this SPIA addresses issues or risks in relation to the energy CDR that have not been identified as issues or risks in the CDR PIA. These issues arise, for example, due to the designation of the Gateway, the proposed authentication models the proposed Priority Energy Datasets, and the proposed data flows.

c. The CDR PIA provided a detailed overview and description of the CDR and its framework on which this SPIA relies and refers to. They are not repeated in this report, save where they have a direct application to the assessment in relation to the energy CDR. These comprise the following topics:

    i. an overview of the CDR (except for an overview of the CDR regime as it would apply to the energy sector);

    ii. background to the development of the CDR;

    iii. an overview of the CDR legislative provisions in the CCA;

    iv. summary of the draft CDR Rules (except for any relevant changes in the CDR Rules);

    v. summary of the draft Consumer Data Standards, including the CX Standards and the CX Guidelines (except for any relevant changes since the July 2019 working draft);

    vi. data flows between participants in the CDR (except to the extent these relationships differ in the energy sector and based on the AEMO Gateway Model preferred by the ACCC); and

    vii. mapping the Australian Privacy Principles (**APPs**) in the *Privacy Act 1988* (Cth) (**Privacy Act**) against the CDR Privacy Safeguards and highlighting any differences between the two in relation to application and substance (except to the extent the CDR Privacy Safeguards apply to a Gateway).

d. In performing this SPIA, the following steps were performed:

    i. **Initial briefing**: we were briefed by, and consulted with, Treasury and the ACCC and agreed on the scope of this SPIA and working assumptions, which were refined during the assessment. We also discussed and identified the stakeholders to be approached, material to be relied on and confirmed the timeframes for completing this SPIA;

    ii. **CDR PIA and the Treasury's response**: we reviewed the CDR PIA and its explanation of how the CDR would apply in Open Banking as well as the CDR Data flows, key privacy risks and recommendations and those which Treasury has confirmed will be implemented in its agency response having regard to the objectives of the CDR;

    iii. **CDR Rules**: we reviewed the CDR Rules, which have now commenced. The CDR Rules have been designed so that they will apply economy-wide, but it is also intended that the CDR Rules will be

[15] OAIC's *Guide to Undertaking Privacy Impact Assessments*, 5 May 2014.

amended to deal with specific provisions that will apply only to certain classes of product data and consumer data for different designated sectors, having regard to the sector's particular features;

iv. **CDR Privacy Safeguard Guidelines**: we reviewed these guidelines which outline how the OAIC will interpret and apply the 13 CDR Privacy Safeguards in the CCA when exercising its functions and powers in relation to the CDR;

v. **Stakeholder consultation**: this is an important element of a PIA. In conducting this SPIA, a range of target stakeholders were identified and consulted, including relevant government departments and agencies, a selection of Electricity Retailers across the market, energy and water ombudsmen, consumer representatives, and the AEMO. These stakeholders provided valuable insights into potential complexities arising for the energy CDR. A list of stakeholders is provided at **Appendix 4** to this report and their feedback is reflected in this report;

vi. **Publicly available information**: this SPIA draws on and reflects a range of publicly available and relevant submissions, reports and papers, including applicable research which were reviewed in the time available. A list of key materials that have been considered during the development of this SPIA is included in **Appendix 3** to this report;

vii. **Consumer Data Standards**: we considered the applicable technical standards that were relevant to formulating our analysis in this report;

viii. **CX Standards and Guidelines**: the objective of the CDR is to enable consumers to participate seamlessly in the CDR environment and to access and understand the CDR Data that is held about them. We considered the applicable CX Standards and Guidelines that were relevant to formulating our analysis in this report;

ix. **Energy sector's regulatory framework and energy data**: we considered the overarching regulatory framework of the energy sector and the key relevant energy participants and data collection and transfer processes;

x. **Privacy impact and compliance analysis**: we identified and critically assessed and analysed the potential privacy impacts and risks from the proposed designation of the energy CDR based on the Priority Energy Datasets, the AEMO Gateway Model, the proposed authentication models, the anticipated data flows and the CDR participants identified by Treasury. We noted the findings from the CDR PIA, stakeholder feedback, the current status and understanding of the energy CDR, and the application of the CDR legislative framework to the energy sector. Consistent with the CDR PIA, we have not attempted at this stage to attribute a risk level or rating to the privacy risks we have identified in this report. Stakeholders with whom we discussed this SPIA agreed with this approach. Our recommendations were developed on this basis;

xi. **Recommendations**: we identified and considered potential risk mitigation strategies that could further address the privacy risks and their likely effectiveness in removing or reducing avoidable risks. We also considered whether they were feasible at the current time or at some stage in the future before the commencement of energy CDR;

xii. **Draft report**: we prepared the draft report and submitted it to Treasury and the ACCC on 27 April 2020 for review and feedback. Relevant feedback from Treasury and the ACCC has been incorporated in this report;

xiii. **Report**: we finalised this SPIA and submitted this report to Treasury on 25 May 2020; and

xiv. **Review of and response to final report**: we understand that Treasury and the ACCC may further consult with stakeholders as required to respond to the recommendations and at some stage this report may be updated or supplemented.

Part 7. Energy CDR and its Key Features

This section of this report supplements the CDR PIA by including the key concepts of the CDR that are relevant to the energy sector, and providing context to support an understanding of the findings in this report.

7.1 Energy sector structure and regulatory frameworks

In order to assess the privacy impacts and risk mitigation strategies for the designation of the CDR in the energy sector, it is important for context to understand in general terms the current structure and regulatory environment of the energy sector. These impact the way the proposed CDR participants operate and engage with consumers and how the Priority Energy Datasets for the energy CDR will flow, noting these are complex and the subject of ongoing reform.

a. **Development of the NEM**

Energy is an essential service that is of critical importance to everyone. Traditionally, energy assets were government-owned and operated but the supply of energy (i.e. electricity and natural gas) has increasingly evolved into a privatised and competitive market in Australia since the end of the 1990s. The establishment of the NEM in 1998 in five physically connected States and Territories involved the creation of three market entities (the Australian Energy Market Commission (**AEMC**) and the Australian Energy Regulator (**AER**) which is part of the ACCC in 2005,[16] and the AEMO in 2009.[17] The NEM was also underpinned by an agreement to allow for national legislation, the National Electricity Law (**NEL**),[18] to be implemented in participating Australian States and Territories.[19] The NEL is supported by the National Electricity Rules (**NER**).

b. **Transmission of electricity**

The NEM provides the wholesale market for registered participants such as generators and retailers across the country to generate, transmit, connect, distribute and trade electricity that is generated for the grid (with the exception of Western Australia and the Northern Territory, which have separate systems and regulatory arrangements and to which the energy CDR will not apply at this stage). The NEM is responsible for the delivery of approximately 80% of national electricity consumption, and hence, captures a wide number of electricity consumers.[20]

Generation of electricity comes from both traditional and newer renewable sources of energy and is coordinated by the AEMC. Generators of electricity are interconnected through complex transmission networks operated by transmission network service providers, and from then through distribution networks (the poles and wires for electricity) operated by distribution network service providers to consumers. Electricity distributors own and manage the poles and wires through which electricity is delivered.

The transport of electricity from generators to consumers is facilitated through a 'pool', or spot market, where the output from all generators is aggregated and scheduled at fixed intervals to meet demand. Currently this is set at 30 minute intervals, but this will change from 1 July 2021.[21] The NEM instructs

[16] The AEMC was established under the *Australian Energy Market Commission Establishment Act 2004* (SA); AER was established through the *Trade Practices Amendment (Australian Energy Market) Act 2004* (Cth) and now operates under the CCA.
[17] The AEMO was established under the *Australian Energy Market Amendment (AEMO and Other Measures) Act 2009* (Cth).
[18] The NEL appears in Schedule 1 to the *National Electricity (South Australia) Act 1996* (SA) and applies to each jurisdiction in the NEM through individual enactments of the national scheme.
[19] By the *Australian Energy Market Act 2004* (Cth).
[20] See the AEMC's webpage "National Electricity Market", retrieved 27 April 2020.
[21] See the AEMC's webpage "Five Minute Settlement", retrieved 5 May 2020.

generators how much energy to produce at each interval so that the supply is matched to consumer requirements and the current energy price for pooled or spot energy can be calculated. This is managed by AEMO through a series of technical procedures according to the NEL and NER.

c. **Metering**

Historically, properties in Australia were connected to the electricity market via a meter installed at the premises. These meters were known as 'accumulation meters' or 'interval meters'. Accumulation meters would register only the total electricity used as it passed through the meter. This means that a consumer would not be able to understand when throughout the day electricity was consumed, and when it might be cheaper to use electricity consuming appliances to receive lower rates and ultimately a lower electricity bill.

Interval meters are capable of measuring electricity usage to the 30-minute interval. This provided a consumer with more data about when they were consuming electricity and to assist retailers to better understand a consumer's usage pattern. This helped pave the way for a broader spectrum of electricity service plans that provided different rates for electricity consumption depending on the time of day. This also led to competition among Electricity Retailers to develop tailored and useful plans for electricity consumers.

Within the last decade, 'smart meters' have been installed in many Australian homes.[22] These meters record electricity usage at every 30-minute interval and the data can be shared remotely with the electricity distributor on a more frequent basis than before. Generally, the electricity distributors are responsible for installing and maintaining the smart meters. This helps improve billing accuracy, promotes competition in the electricity retail market and provides more options to consumers to enable better decisions to be made in relation to their electricity service plan.

d. **National Energy Customer Framework (NECF) and Victorian Energy Retail Code (VERC)**

The National Energy Customer Framework (**NECF**) is the retail regulatory scheme for the NEM that was introduced in 2011 to provide consumers with a range of protections based on the recognition that energy is an essential service. It comprises the National Energy Retail Law (**NERL**)[23], the National Energy Retail Regulations and the National Energy Retail Rules and is governed by the AER and operates alongside the Australian Consumer Law (**ACL**). Once the CDR is designated to the energy sector, there will be two data access regimes operating simultaneously.

The NECF regulates the connection, supply and sale of energy (both electricity and gas) to residential and small business customers who are connected to the grid. The protections it provides relevantly cover activities such as:

i. how retail offers must be presented and disclosed;

ii. notification about discounts ending, tariff changes and meter readings;

iii. the requirement to obtain explicit informed consent from consumers before entering into agreements to transfer energy retail services to a prospective retailer or to establish a new agreement with an existing retailer; and

iv. provisions for vulnerable customers, such as a prohibition on disconnecting life support customers and the requirement for retailers to establish a Hardship regime.

[22] From 1 December 2017, any new or replacement meters for residential properties and small business commercial properties will be smart meters.
[23] The objective of the NERL is in item 13 of Schedule 1 to the *National Energy Retail Law (South Australia) Act 2011* (SA): "to promote efficient investment in, and efficient operation and use of, energy services for the long term interests of consumers of energy with respect to price, quality, safety, reliability and security of supply of energy".

Victoria did not adopt the NECF and its electricity retail market is currently regulated by the Essential Services Commission (**ESC**). It has undergone a process of harmonisation with the NECF (subject to some exceptions) through the adoption of the VERC which provides a range of similar consumer protections. The existing data access regime under the NECF is discussed further in this report.

e. **Power of Choice reforms**

The *Power of Choice* reforms is a package of reforms that are designed to give customers more options for and control over how electricity is used and managed. These reforms were initiated following the AEMC's Power of Choice review in 2012 to support demand side participation to enable better network pricing arrangements and to arm consumers with more information about electricity consumption to make better decisions. Some of these reforms have assisted to:

i. enable the competitive deployment of smart meters across properties located within the energy sector;

ii. reduce barriers to embedded network customers accessing better plans and offers from Electricity Retailers; and

iii. introduce competition in metering services, to enable greater uptake of advanced metering technology.

f. **Distributed Energy Resources (DERs)**

Distributed generation units (e.g. small generation and electricity storage devices) are installed on the consumer side through which customers generate their own power using solar panels, energy efficient devices, and residential battery systems. While electricity delivered by the main electricity grid is 'in front of the meter', these DERs are 'behind the meter' and represent the ways more electricity customers are taking control of their production and use of electricity to have it supplied directly to their home without the need to go through an electricity meter.

On 1 March 2020, the AEMO launched the DER Register. The development of this register followed the AEMC's amendment in late 2018 to the NER, enabling the AEMO to establish a register to improve the visibility and access to essential DER device information across Australia. The source of the DER Data will be the DER Register. There is a risk that Personal Information could be collected about third parties, including DER installers and electrical contractors, and ultimately disclosed to Accredited Persons.

g. **Current energy data access frameworks**

Energy consumers in the energy sector have existing rights under the NERL to request access to information about their energy product and pricing in the form of pricing and product disclosure / information statements and to request copies of their bills, which contain a range of mandatory information including details about their consumption, pricing, Concessions and discounts.[24] For example, under rule 28 of the National Energy Retail Rules, an Electricity Retailer must promptly[25] provide a small customer[26] with historical billing data for the previous two years (on request) and under rule 56A of the National Energy Retail Rules, an Electricity Retailer must provide a small customer or representative with

[24] We have not undertaken a review of the NECF and the VERC in detail given the scope and objective of this SPIA. However, we flag relevant aspects of the NECF and the VERC to contextualise our analysis.
[25] For Victorian retailers, rule 28 of the Victorian Energy Retail Code (version 15, 2 February 2020) requires best efforts to provide this information within 10 business days.
[26] For example, a residential consumer or a small business. See, specifically, section 5 of the *National Energy Retail Law (Queensland) Act 2014* (QLD) for the definition of 'small customer'.

information about the customer's energy consumption for the previous two years.[27] Additionally, individuals have access rights to Personal Information held about them by an Electricity Retailer under relevant privacy legislation.[28]

In addition, the regulatory bodies in the energy sector have taken steps as discussed in this report to enhance the accessibility of consumers to energy data. For example, the AEMC made a ruling on 1 December 2014 that expanded on existing rights of consumers to access historical electricity consumption data including provisions for customers to nominate authorised representatives to request data on their behalf and a requirement that Electricity Retailers and distributors comply with formatting requirements as far as how the information is presented.

Authorised representatives of the primary account holder also have the ability to request consumer energy data from the Electricity Retailer. Clause 7.15.5(d) of the NER enables an authorised representative of the customer to make a request for access to energy data in accordance with the metering data provision procedures described in rule 7.14 of the NER. This existing process recognises that individuals other than the primary account holder may access energy data where they have the appropriate authorisation.

7.2 Energy sector participants

Energy regulation has become increasingly complex in recent years, as the number of government agencies and organisations who play an active role in the energy sector has increased. As well as the AER and ESC's regulatory frameworks, there have been a range of Commonwealth and State-based reviews and enactments.[29] The NEM currently has about 300 registered participants and supplies electricity to approximately nine million customers. The roles of the following energy participants are relevant to this SPIA.

a. **AER as operator of Energy made Easy (EME)**

The AER operates under the CCA and regulates the NEM's retail sector and is required to monitor, investigate and enforce compliance with obligations under the NERL. The AER publishes guidelines which prescribe enforceable requirements for regulated businesses and conducts reviews that promote the long-term interests of electricity and gas customers.

EME is a free government online service operated by the AER that helps residential and small business energy consumers navigate the retail markets to find a suitable energy offer. The AER's role is to collect retail product data from Electricity Retailers, which it has the power to do under the NERL, and in accordance with its *Retail Pricing Information Guidelines*.[30] The AER provides Electricity Retailers with access to a secure online portal, through which they must provide Generic Product Data to EME.

b. **Victorian's Essential Services Commission (ESC)**

The ESC regulates Victoria's retail energy sector and is required to monitor, investigate and enforce compliance with obligations under the VERC. The ESC publishes codes and guidelines which prescribe enforceable requirements for regulated businesses. The ESC also conducts reviews and inquiries that promote the long-term interests of electricity and gas consumers.

---

[27] See also rules 86A and 86B of the National Energy Retail Rules.
[28] See, for example, APP 12 under the *Privacy Act 1988* (Cth), section 14 of the *Privacy and Personal Information Protection Act 1998* (NSW), and Information Privacy Principle 6 under the *Privacy and Data Protection Act 2014* (Vic).
[29] For example: the ACCC's Retail electricity pricing enquiry 2017-18, leading to the AER's establishment of a Default Market Offer; the ACCC's amendments to the CCA to prohibit energy market misconduct; and, the Victorian Government's Independent and Bipartisan Review of the Electricity and Gas Retail Markets, leading to the implementation of a Victorian Default Offer.
[30] The latest version of the AER's Retail Pricing Information Guidelines is version 5.0, 31 August 2018.

c. **Victorian Energy Compare (VEC)**

VEC is an independent Victorian Government energy price comparison site operated by the Department of Environment, Land, Water and Planning (**DELWP**). It is designed to help compare electricity offers from all Electricity Retailers, based on information that is provided by households or small businesses. The VEC operates by collecting data from participating Electricity Retailers who submit Generic Product Data to VEC. The VEC then uses this data together with data volunteered by the consumer to provide a comparison of products based on price, scope of offer, discounts and other metrics of importance to electricity consumers.

d. **Electricity Retailers**

There are approximately 30 Electricity Retailers operating in the NEM.[31] Electricity Retailers collect data from their customers to enable the provision of electricity services. Data collected from customers includes Customer Provided Data. Electricity Retailers will also have information about the plans that are available and any specific aspects of the plan that can be tailored to suit the customer's requirements. Electricity Retailers are required to have Hardship policies in place and to advise customers on how to access energy Concessions, relief schemes or energy rebates that they may be eligible for.

We consulted with two Electricity Retailers of varying size and market share.[32] Both organisations confirmed that they have privacy and information security frameworks to support the secure and effective use of Personal Information during their operations. They indicated that they are yet to receive further clarification about the design of the energy CDR so that they can begin implementing steps to develop processes to comply with the energy CDR. At present, both Electricity Retailers confirmed that they are aware of the CDR, have taken steps to plan to implement the CDR and are actively engaged in reviewing developments to the energy CDR.

e. **Australian Energy Market Operator (AEMO)**

The AEMO is responsible for managing the supply of energy to Australian households and businesses and operating the financial markets that allow energy to be bought and sold. This role requires access to data to enable the AEMO to make accurate and timely decisions about the generation, transmission and distribution of energy. The AEMO collects data from various energy sector participants including Electricity Retailers and electricity distributors.[33]

The AEMO also operates the retail markets across the NEM which underpin the wholesale markets. These operations facilitate competition among Electricity Retailers to enable customers to purchase an electricity service from an Electricity Retailer of their choice. This allows customers to choose which service provider they go with based on available information, plans and offers and any tailoring offered by the Electricity Retailer.

The AEMO has established the B2B eHub which is an electronic exchange platform that it provides, operates and maintains to facilitate B2B communications by energy sector participants. The B2B eHub does not give the AEMO access to that data. The AEMO is currently investigating what technology solution will best support the data access model for the CDR in the energy sector.

[31] See the AEMC's webpage "Spot and Contract markets", retrieved 27 April 2020.
[32] We had planned to consult with a third Electricity Retailer. However, due to circumstances beyond our control, this consultation did not proceed.
[33] In addition, the AEMO manages the DER Register (effective from 1 March 2020).

7.3 Privacy regulatory framework for energy sector participants

a. Participants in the energy sector must handle and process personal information across its lifecycle (which includes its collection, use, disclosure, quality, transparency, storage, disclosure, de-identification and security) in accordance with applicable Commonwealth and State / Territory-based information privacy laws.

b. The Privacy Act protects the handling and processing of Personal Information that is collected and held by Commonwealth agencies and private 'organisations' who are not subject to the 'small business' exemption as they have an annual turnover of more than AUD$3 million.[34] The entities must comply with the APPs set out in Schedule 1 to the Privacy Act (**APP entities**). An act or practice of an APP entity in relation to Personal Information that breaches an APP or the notifiable data breach scheme in Part IIIC of the Privacy Act is an interference with privacy and may be subject to a complaint or regulatory action by the Australian Information Commissioner through the OAIC. The energy sector participants that must comply with the APPs are the AEMO, AER (including EME), Electricity Retailers and any privately owned comparison sites.

c. The Privacy Act does not generally apply to local, state or territory based government agencies. However, these agencies must comply with state and territory privacy and data protection laws that apply to public sector agencies. The Victorian agencies such as the DELWP (including VEC) and ESC who are subject to the *Privacy and Data Protection Act 2014* (Vic) must comply with the Information Privacy Principles set out in Schedule 1 and the AEMC, which is an independent South Australian statutory body, is subject to South Australian Information Privacy Principles Instruction.

d. In addition to the Commonwealth and State / Territory privacy law regimes, the NERL and the VERC require Electricity Retailers to obtain the customer's explicit informed consent (either in writing or orally, including electronically) prior to engaging in a transaction that involves the provision of an electricity service from the same Electricity Retailer or the transfer of an electricity service from a different Electricity Retailer. A record of this consent must be stored by the Electricity Retailer for at least two years.[35]

[34] See definitions in sections 6, 6C and 6D of the Privacy Act.
[35] See, for example, Division 5, Part 2 of the *National Energy Retail Law (NSW) 2012* (NSW).

7.4 Priority Energy Datasets

This table sets out the six Priority Energy Datasets as well as the Gateways and Data Holders that Treasury proposes at this stage will be subject to the Designation Instrument for the energy CDR.[36]

	Data set	Details	Data Holder	Gateway
Customer data	Metering Data	Usage data from type 4-6 meters, and potentially type 1-3 meters.	AEMO	N/A[37]
	NMI Standing Data	Information including Average Daily Load, meter installation type, network tariff code and presence of a controlled load.	AEMO	
	Distributed Energy Resource (DER) Data	Information about solar panels, batteries and other DERs.	AEMO	
	Customer Provided Data	Information that identifies the CDR Consumer including the name, contact details, date of birth, property address, controlled loads and billing information.	Electricity Retailers	AEMO
	Billing Data	Information including records of bills issued, payments received, and payment arrangements.	Electricity Retailers	
	Tailored Product Data	Information about the plan the customer is on and any specific features tailored to the customer.	Electricity Retailers	
PRD	Generic Product Data	Generally available information about the plan customers are on.	Electricity Retailers	Potentially, Energy Made Easy (of the AER) and Victorian Energy Compare (of the DELWP)

7.5 Key features and privacy considerations for data access in the energy sector

There are a number of key features of the energy sector which need to be considered in the context of how they influence the types of impacts and risks that may arise for energy consumers (compared to the consumers in Open Banking). These include the different ways in which consumer data within the energy sector is associated, understood, shared and used and how consumers engage with their data and with energy participants. The potential sensitivity of energy data has been assessed at a point in time based on feedback from stakeholders about how the data is currently being used and how the data might be used in the energy CDR when it is collected by Accredited Persons and used to offer goods or services to CDR Consumers. The key features and concepts relevant to privacy considerations in the energy CDR are detailed below.

[36] Treasury's Priority Energy Datasets Consultation, CDR, 29 August 2019. Tailored Product Data and Generic Product Data collectively referred to as Product Reference Data (PRD), and constitute one dataset. We note that the draft *Consumer Data Right (Energy Sector) Designation 2020* released by Treasury on 6 May 2020 for consultation may update the contents of the table in **Section 7.4** of this report.
[37] We understand that where the AEMO is a Data Holder, it will not technically deliver that data via itself as a Gateway. However, in practical terms, we expect that the AEMO is likely to deliver the data it holds, and the data it transmits from other parties, together as a single data packet.

a. **Energy consumption data (i.e. Metering Data)**

Energy is generated, transformed, pooled, transmitted, distributed and delivered for consumption at premises by individuals and organisations through a complex series of systems and procedures. Consumption of electricity by a premises is measured by the electricity meter situated at the premises through which electricity must pass. The consumption of electricity has a significant impact on the overall cost payable by the account holder for the service. In addition, the cost might be affected by DERs situated at the premises which produce electricity and sit 'behind the meter'.

Metering Data is a Priority Energy Dataset. It is defined as energy usage data from type 4 to 6 electricity meters, and potentially from type 1 to 3 electricity meters. Meter types 1 to 3 are meters for large customers, and types 4 to 6 are meters used by households and small businesses (smart (Type 4) meters, interval (Type 5) meters, and also accumulation (Type 6) meters). All type 4 to 6 meters record how much energy is used over a period of time, but accumulation meters cannot record what time of day. The type of meter can influence how a retailer may charge for usage (e.g. single / flat rate or time of use).[38]

The collection, management and distribution of Metering Data across the NEM is a collective process which is regulated by the metrology and metering procedure documents which the AEMO is responsible for. MDPs are the parties responsible for the collection and distribution processes on behalf of other market participants and bodies, including both the relevant Electricity Retailer and the AEMO. The details of metering installation and minimum specifications are set out in the *Metrology Procedure: Part A* and the processes of metering data validation, substitution and estimation are set out in detail in the *Metrology Procedure: Part B*.[39]

Smart meters communicate this data directly and provide actual and real-time consumption data replacing manual and estimated readings that otherwise take place. They also allow for more flexible electricity pricing as different tariffs can be charged at different times of the day. Data from meter readings are required by Electricity Retailers for billing purposes, when consumers change retailers or when power is re-connected to a premises such as when a customer moves house. The data is validated in the distributors' systems and then sent to Electricity Retailers for the purpose of calculating the customer's bill.

An energy customer who is responsible for an account and who receives and pays the electricity bill will not always be the only individual who consumes the electricity at the premises to which the electricity is delivered, or may not consume the electricity at all. This is because the account holder might have leased the premises out to tenants, the account holder resides overseas and the property is occupied by his or her family, or the account holder is a small business owner where the property that operates the business is occupied by his or her employees on a daily basis.

While the account holder is the person financially responsible for paying the bills and managing the electricity service with the Electricity Retailer, due to the shared nature of energy usage data and the account holder arrangements, concerns were raised by stakeholders that NMI Standing Data and Metering Data may reveal consumption patterns, indication of timing of household presence and other information that may identify the individual occupying a premises. Where occupiers of premises change over time but the account holder does not, the number of individuals who may be engaged in the consumption of electricity increases. This data may become CDR Data of the account holder as an Eligible CDR Consumer, but the individuals may not be aware or be notified of the transfer of this data. These individuals may have an interest in accessing and knowing about their energy consumption and costs (e.g. should the account holder on-charge the costs to the occupants either on a fixed or variable basis).

Stakeholders acknowledged that while the risk of identifying or inferring insights about another individual who is not the CDR Consumer will be amplified due to the CDR, the risk already exists. While stakeholders

[38] There can also be controlled load (or dedicated circuit) tariffs for nominated appliances and will depend on the applicable energy network.
[39] Both of these documents are available at the AEMO's website.

noted that there have been attempts to find out whether an individual is living at or using a premises by, for example, purporting to wish to settle an electricity bill, for which Electricity Retailers had measures in place to manage, no stakeholder could specifically point to an example of where Metering Data itself would be capable in their proposed current form (including historical Metering Data) of identifying, enabling the compilation of insights about or allowing a profile to be built about an identifiable or reasonably identifiable individual who is not the CDR Consumer.[40]

The risk of identifying an individual is lessened when multiple occupants reside at the property and electronic devices are being used that consume nominal amounts of electricity to operate while active or on standby (e.g. computers, alarm systems, security camera systems, solar panels, automatic heating / cooling and lighting). To be able to identify any individual occupant or energy user with reasonable certainty based on Metering Data alone (and without any other smart home devices, sub-metering or circuit-level analysis) would, in our opinion, be difficult. After consulting with stakeholders and adopting the threshold test of the definition of Personal Information in the Privacy Act, at this point in time there is no reason to conclude that these individuals would be reasonably identifiable to an ADR from Metering Data (as currently defined). This means, therefore, that no potentially sensitive information would be disclosed about them. There is a risk that together with others types of information, the data collectively may identify or reasonably identify a person.

As the scope of the energy datasets widens in the future (i.e. beyond the Priority Energy Datasets) and the more real-time granular data that smart meters provide, this risk may materialise and impact on individuals.[41]

b. **NMI Standing Data**

NMI Standing Data is a Priority Energy Dataset. The AEMO will be the Data Holder for this dataset. Each connected meter to the NEM has a unique 10 or 11 digit NMI. This enables Electricity Retailers to identify and match a customer's connection to the right electricity account and collect meter usage data at the supply address. Properties with separate metering such as apartment blocks may have more than one meter and NMI. A NMI is also required for switching retailers and submitting individual meters reads (including where an estimated read is required). The NMI associated with the property linked to the account will be made available on a customer's bill.

The NMI does not move with a customer unlike for a bank account where the banking data is more closely connected to the individual and their personal transactions (such as payments or receipts). Bank accounts and bank customers and the account and customer numbers at their point of creation, are generally associated with one legal entity i.e. one or multiple private individuals or a business. They cannot be re-assigned over time to others, whereas the NMI remains at a property for as long as the land on which the property is registered does not become subdivided or merge with other parcels of land.

The management of electricity supply, by comparison, works in such a way that one NMI can and will be attributed to different legal entities over time, for example, when properties change ownership, tenants move homes, and business entities restructure. Given that the scope of the Priority Energy Datasets anticipates the inclusion of historical energy consumption data, energy participants will need to be equipped with adequate systems and data management processes to effectively quarantine information on an entity-to-entity (customer to customer) basis and in many cases identify when the electricity service account was created and when the entity took possession of the property.

[40] We note that a similar view was shared by the author of the PIA commissioned by DELWP in relation to Advanced Metering Infrastructure released in August 2011.
[41] We note that the author of the PIA commissioned by DELWP in relation to Advanced Metering Infrastructure (released in August 2011) foresaw a similar risk based on the increased richness of data produced by smart meters.

Like Metering Data, NMI Standing Data will include information that is relevant to the meter, the presence of controlled loads and the tariff attributable to a property depending on the consumer's profile. After consulting with stakeholders, at this point in time there is no reason to conclude that this type of data alone is likely to reasonably identify or identify an individual. As for Metering Data, this is because more than one individual is residing in a property and also the AEMO only holds the NMI and NMI address (which does not include the contact details or identity of the current account holder). Although the NMI will also have a NMI address attributed to it, and the location of the NMI could be pinpointed on a geographical map, there was no indication through stakeholder discussions that it could disclose the identities of the individuals residing at the property. Again, together with others types of data, it may collectively identify or reasonably identify a person.

c. **DER Data**

DER Data comprises data collected by the AEMO through its DER Register.[42] From 1 March 2020, installers of DERs are required to submit information for the purpose of populating the DER Register. Under the NER, the AEMO is required to report on the DERs located in the NEM. The purpose of the DER Register is to ensure that the locations and specifications of all DERs connected to the NEM are known so that the AEMO can manage the reliable and secure supply of electricity to consumers connected to the NEM. In addition, this information will assist innovation in electricity markets for consumers who use DERs to ensure the effective integration of all DERs into the NEM.

The DER Register will collect 13 pieces of additional information about DER equipment installed at a property.[43] This information will be supplied by the installers of the DER device and submitted to the electricity distributor for incorporation into the DER Register. Information, including what has been installed on site, such as the device, serial number, installation type and connection points, together with information from the Clean Energy Regulator's approved product database, will be stored in the DER Register. The *DER Register Information Guidelines* published by the AEMO provides further information about the handling, storage and security of the data held in the DER Register.[44]

While the data collected by the DER Register relates to the NMI, type of equipment installed and the installation performed, the data is in our view unlikely to identify or reasonably identify an individual (unless the consumer's or installer's Personal Information is included in the data). Clause 3.7E(h)(2) of the NER requires the AEMO to have regard to the confidentiality and privacy of an individual in relation to the inclusion of information in the DER Register. While the AEMO may include "other data" as per section 3.3 of the *DER Register Information Guidelines*, it will need to comply with the NER in doing so. This provision in the NER may prevent information about the consumer and installer of the DER being stored in the DER Register. However, controls will need to be implemented (based on rules for the energy CDR) to avoid this disclosure occurring.

d. **Customer Provided Data**

Customer Provided Data includes data held by Electricity Retailers about the individual who holds the account, including any joint account holder information and information about authorised representatives. This dataset will ordinarily include information about an individual that may or will identify an individual. Information forming part of this dataset includes the individual's full name, email address, contact information, date of birth, postal or billing address and account number.

Since the Accredited Person will be engaged by the individual making a Consumer Data Request, and the individual will be authenticated prior to the disclosure of this data by the Data Holder to the Accredited

[42] We have not undertaken a deep analysis of the DER Register. We understand that the information collected by the DER Register will include DER generation information, demand side participation information and other data provided by any person to the AEMO.
[43] See the AEMO's webpage "Distributed Energy Resource Register", retrieved 4 May 2020.
[44] The AEMO's DER Register Information Guidelines, version 1.0, 2 September 2019.

Person, this should avoid an individual improperly obtaining access to data about another individual without their authorisation. Based on the ACCC's proposed authentication models, we have assessed the risks in **Part 8** of this report.

e. **Billing Data**

Billing Data is produced by Electricity Retailers. The data is based on Metering Data and NMI Standing Data. This datasets will contain information about bills issued, record of payments received and any payment arrangements. By its very nature, billing data will be historical data. As previously noted, there is already a process to access this historical billing data (up to two years' worth) under the NECF and the VERC for free and beyond two years for a charge. After consulting with stakeholders, Billing Data on its own and as defined at this point in time will not, in our reasonable opinion, be capable of revealing the identity of an individual. Again, together with others types of data, it may collectively identify or reasonably identify a person.

Through stakeholder consultations, we understand that Electricity Retailers do not typically hold information about whether an individual is on a Hardship plan or the recipient of a Concession in the same database as the billing database (or equivalent). While we have not consulted all Electricity Retailers to understand their individual information management practices, it appears that Electricity Retailers may need to ensure that the Billing Data, as defined in the Designation Instrument, effectively quarantines information in relation to an account holder's sensitive arrangements, for example, Hardship plans, Concessions, family violence arrangements, and life support provisions.

To strike an appropriate balance between the privacy impacts of disclosing Billing Data and providing the ability to ADRs to offer the best products and services to CDR Consumers, the Accredited Person will need to be clear about what information it needs from the Data Holder. To the extent that information about a Hardship plan or Concession is required to tailor them for the CDR Consumer, this information may be requested in accordance with the Data Minimisation Principle. It is unlikely, in our opinion, that information about family violence arrangements and life support provisions will be needed by ADRs when providing a good or service because, for example, the latter type of information is already held in life support registers available to Electricity Retailers.

We consulted with some stakeholders about whether a person could be identified as being on a Hardship plan or the recipient of a Concession, based solely on the amounts paid over a period of time. We understand that, while the data could be reverse engineered to determine this, it would be a difficult process because Hardships plans are specific to the Electricity Retailer, individuals might be on a payment plan not due to Hardship, and an electricity customer's bill varies over time since consumption is never constant.

f. **Product Reference Data**

Comprising Generic Product Data and Tailored Product Data, PRD refers to data about the product offered by the Electricity Retailer to consumers. At present, EME (hosted by the AER) and VEC (hosted by DELWP) are examples of product comparison websites providing Generic Product Data that allow consumers to compare products offered by Electricity Retailers based on information volunteered by consumers into the system and product data supplied by participating Electricity Retailers. The CDR will include this type of information so that it can be disclosed to Accredited Persons to help them provide a good or a service that will benefit the CDR Consumer.

Unlike Generic Product Data, which will contain product plan information provided by an Electricity Retailer that is publicly available or available for anyone to enquire about with an Electricity Retailer, Tailored Product Data may include additional information that is specific to a consumer or a group of electricity consumers. The specific data packets to be included in this type of dataset is yet to be defined. When we discussed this

dataset with stakeholders, they were not able to provide specific comments due to uncertainty about what information would be included in this dataset.

g. **Data quality**

There are a range of existing data quality issues in the energy sector that are inherent features of the industry. Although one stakeholder expressed the view that the accuracy of energy data is not an issue, rather the scheduling, frequency and validation, which is set by the AEMO under the NER. It is not expected that these existing issues will be changed immediately for the purposes of the energy CDR.[45]

It is likely that the CDR may amplify quality issues with the uptake of Consumer Data Requests, but this may also present an opportunity to address the issues, as attempts to deal with these by energy participants continue. Some solutions to resolve these issues have been identified as a timely and costly remediation exercise. These issues are known to affect the currency, accuracy, quality and security of data including, from time to time, the:

i. misalignment between the address as known to the consumer and / or premises owner compared to the address attributed to the NMI, caused by factors including:
    a. outdated address recorded in MSATS;
    b. customer errors such as providing the correct street address but incorrect suburb to the Electricity Retailer;
    c. administrative keying errors when establishing new meters; and
    d. the absence of an obligation to proactively and regularly validate metering database addresses to reflect changes to council or postal address configurations;

ii. misidentification of customers. At present, the AEMO relies on data from other energy participants to identify consumers. While it has NMI Standing Data and NMI addresses, it does not know the customer's personal details such as their name and other identifiers. Therefore the sources of these errors will be Data Holders and also the customers themselves through data they provide to Accredited Persons and Data Holders; and

iii. misalignment between the customer's premises (i.e. where they reside) and the energy supply they are paying for, caused by factors including:
    a. cross metering, where the physical meter has the correct NMI for a property, but is not wired to the correct premises (most often found in multi-premise dwellings e.g. apartment buildings); and
    b. erroneous NMI transfers when switching energy retailers or moving home.

The Energy and Water Ombudsmen identified in consultation that a regular complaint received was in relation to the quality of data received. However, upon further investigation, it was also revealed that many consumers of electricity services would not be able to ascertain whether the data they have received is related to the account which they hold. Compared to the datasets in Open Banking, Metering Data for example is more linear, predictable and structured compared to an individual's banking transaction data, and there are fewer opportunities for individual consumers to query the data with an Electricity Retailer and assess whether the electricity bill is correct. The Ombudsmen noted that in these circumstances, they have investigative powers to collect data from energy sector participants to verify, for example, that the customer's bill has been accurately calculated based on the data from the applicable electricity meter.

[45] We understand that participants in the energy sector are aware of these issues and work together to continually develop solutions.

h. **Identity of the CDR Consumer**

In Open Banking, the concepts of an account owner, or joint account owner, is well established, defined and understood. It is generally clear whose Personal Information is being dealt with, what an 'account' is and what products and services are attributed to that account. However, in the energy sector, energy data is dissected and transacted at a NMI level rather than on a unique account or customer level and a NMI can and will over time be attributed to different legal persons. This means it is not always clear who the relevant consumer is and therefore which individual's Personal Information is being handled when an account is being accessed.

While the one-to-one relationship between the bank and the consumer is generally more clearly defined, in the energy sector there are more consumers potentially involved in the consumption and billing of energy, such as the owner of a premises, family members, friends, tenants, employees and other occupiers. The privacy risks of all those affected need to be considered so that adequate privacy protections are put in place.

An energy customer might also experience difficulty understanding whether the data they have received relates to their consumption. It is also often not possible for energy customers to identify data currency or accuracy issues that relate to their identity and the account to which it is connected over time. While Metering Data may reveal patterns of behaviour, no serious concerns were raised by stakeholders about persistent risks that have arisen save in the context of family violence situations.

Details relating to the household's consumption profile (e.g. the time of day when usage is highest, benchmarking of total usage based on number of occupants) rarely leads to a consumer identifying that the retailer profile is not a match for their circumstances and prompting further investigation. Open Banking consumers, by comparison, are more regularly engaged with the data relating to their banking products and in reviewing their account activity. Transactions by their very nature are so specific that unfamiliar entities or amounts that may appear are easily identifiable. The awareness of the direct financial risks and consequences in the case of unauthorised transactions is much higher and better understood. This creates circumstances where the energy consumer might receive data that is not related to them.

i. **Data sensitivity**

While most energy data may not fall within the definition of Personal Information that is considered 'sensitive information' for the purposes of the Privacy Act, the consensus among stakeholders was that there are certain types of data that consumers would consider to be sensitive to them and they would be concerned about sharing it under the CDR, including for fear of discrimination.[46] There was also consensus that energy data did not generally have the same sensitivities as banking data. Examples of sensitive information to an energy consumer may include information about their ability to pay for the service, a family separation arrangement or health information if an occupant of the household requires life support equipment. Further, vulnerable customers (including those who do not understand English well, are experiencing Hardship or relying on government support) are also less likely to understand the impact of a request to share these types of data with ADRs.

Energy consumers are eligible for a range of retailer assistance programs (e.g. a program from the Electricity Retailer's Hardship regime), exceptions from usual processes and Concessions based on certain personal circumstances. This data may be explicitly or indirectly captured by the Priority Energy Datasets (e.g. Customer Provided Data and Billing Data) including: financial hardship and payment arrangements, difficulty paying for energy costs or paying on time, customers who require life support equipment in their home and concession card holders, including those receiving an aged or disability pension. Retailers must

[46] We note that the analysis in **Section 7.5(i)** of this report is in addition to the analysis of the Priority Energy Datasets described in **Section 7.5** of this report.

have in place approved Hardship and family violence policies,[47] and support consumers with information about Concessions they may be eligible for.[48]

Consultation with stakeholders indicates that Electricity Retailers are likely to have different controls for identifying accounts and consumers with sensitive personal arrangements such as the way they flag accounts and store and share data for such arrangements in a confidential and secure manner (e.g. storing this data in separate databases to Billing Data so that they are subject to access controls). For example, one stakeholder who is a Data Holder noted that their systems which house Billing Data would not reveal whether a customer is on a Hardship program. This is because the databases are separately held and managed by different teams.

Another stakeholder noted that as an Electricity Retailer, it will need to review the data held in particular databases to ensure that the types of data, which are not required to be disclosed to the Accredited Persons, are removed. This includes information dealing with notices to a court or tribunal in relation to family law arrangements. This process will also help to comply with the Data Minimisation Principle and to avoid disclosing unnecessary sensitive information to the Accredited Person. Electricity Retailers often have to deal with attempts by individuals to access data in connection with an account which they are not authorised to access.

A number of stakeholders expressed the view that it would be important for consumers to understand the effect of combining and the potential to derive insights from shared CDR Data that they may consider to be sensitive.

j. **Consumer engagement and literacy**

Given the nature of energy as an essential service and the method by which a consumer's energy consumption is measured and charged, many consumers are currently passively and involuntarily engaged with Electricity Retailers and their consumption and payment for energy. There is a lower incentive to engage and understand their account, their data and the energy participants in the industry because, as we understood from stakeholder consultations, consumers may not be too concerned about their electricity service until something goes wrong. Given the majority of consumers do not understand concepts and terminology used in the energy sector, this discourages electricity consumers to consider matters further.

Other features may impact on a consumer's ability to access the benefits of a competitive energy market. These include a consumer's ability to access technology, their understanding of the market's mechanics and value propositions and the levels of energy market, terminology and digital literacy. Literacy has been consistently raised as a particular barrier in the energy market for vulnerable consumers, including those with no online presence and individuals who do not understand English well. Notwithstanding this issue, one stakeholder who offers electricity services to regional customers did not believe that their customers will be concerned about their inability to participate in the CDR given their offline presence.

7.6 Key concepts for the energy CDR

The CDR PIA explored key concepts of the CDR as it applies to Open Banking. Most concepts apply, except for differences that arise because of the designation of CDR in the energy sector. The following key concepts are referred to in **Part 8** of this report, and this section helps explain these concepts before the concepts are assessed from a privacy risk perspective.

[47] Under the NERL, Electricity Retailer must have approved Hardship policies in place that are monitored by the AER (see, for example, section 43 of the *National Energy Retail Law (South Australia) Act 2011* (SA). In relation to family violence, the VERC was updated in January 2020 to insert new part 3A – assistance for customers affected by family violence.
[48] For example, see clause 19(1)(c) of the VERC.

a. **Eligible CDR Consumer**

Based on the Priority Energy Datasets, an Eligible CDR Consumer in relation to the energy CDR would depend on the meter type that is installed at the property in relation to which they hold an electricity service account, require them to be known to the Data Holder and be the account holder. Other features under consideration are whether they must also be a natural person, may be a joint account holder, must hold an active or open account, must be aged over 18 years and must hold an account that is not restricted to one that can be held online.

At present, only an Eligible CDR Consumer can make a Consumer Data Request. An Eligible CDR Consumer is given further meaning depending on the designated industry to which that consumer belongs. At present, clause 2.1, Part 2, Schedule 3 of the CDR Rules describes who an Eligible CDR Consumer is in relation to Open Banking only. The ACCC will consider what rules are necessary to define the parameters for an Eligible CDR Consumer in the energy sector.

Complexities in the energy sector (as described in this report) will require an appropriate definition of Eligible CDR Consumer in the energy sector to be considered. Electricity account holders may not themselves occupy the premises or may not be the only consumer of electricity at the premises they reside at and which they pay for, for example a landlord of a residential or commercial tenancy, a body corporate or a co-tenant in a shared house. These non-account holders may wish to access CDR Data, and a complexity arises when the occupants of the premises may have changed during the time the account holder has held the account with the Electricity Retailer.

A scenario was considered during stakeholder consultations where a tenant asks the landlord to install an air-conditioning unit and the landlord agrees subject to seeing the impact on energy consumption. The landlord will request data from the Electricity Retailer based on the energy consumption of the occupants. This information may cause the landlord to infer particular behaviours that the tenants might not be comfortable with the landlord knowing.

This tension adds an extra layer of complexity to sharing CDR Data that was not observed in Open Banking. With the application of paragraph 4.12(3)(b) in the CDR Rules, an Accredited Person must not ask a CDR Consumer to give consent to the use or disclosure of their CDR Data if that use or disclosure would identify, compile insights in relation to or build a profile in relation to an identifiable person who is not the CDR Consumer. While this safeguard exists, potential Accredited Person stakeholders who we consulted will need to test further how the Priority Energy Datasets can be used to ensure that it can provides goods or services to CDR Consumers within the parameters of this rule.

In addition, at present, for a person to be a CDR Consumer, the CDR Data must 'relate to' that person and the individual must be identifiable or 'reasonably identifiable' from the CDR Data. This is understood to be broad concept and would include an 'associate' (e.g. a relative or partner)[49] of the individual who holds the account with the Electricity Retailer.[50] This would cover a situation where a member of the account holder's family resides in the property to which the account is linked. The family member or relative may be allowed to process a Consumer Data Request, provided that individual has the requisite authority from the primary account holder when the Data Holder performs the authentication process.

If the individual does not have requisite authority from the primary account holder, the Data Holder will not process the Consumer Data Request as the CDR Consumer has not been successfully authenticated and therefore cannot authorise the disclosure of CDR Data. Through stakeholder consultations, we understand that Electricity Retailers have different approaches to joint account holders and authorised representatives. They may or may not have joint account holders linked to an electricity account and may give authorised

[49] The meaning of 'associate' for CDR purposes has the same meaning as the definition of associate in section 318 of the *Income Tax Assessment Act 1936* (Cth).
[50] See section 56A(3)(a) of the CCA.

representatives varying levels of authority depending on their policy and procedure and the authority granted by the primary account holder.

b. **Authentication**

Authentication refers to the process of verifying that the CDR Consumer that has approached the Accredited Person does hold a valid account with the Data Holder to whom the Consumer Data Request will be made (by the Accredited Person on behalf of the CDR Consumer). This process is key to mitigating the privacy risk of disclosing an individual's Personal Information with an unauthorised third party. In Open Banking, the authentication of the CDR Consumer is performed by the Data Holder. Given the ACCC's preference for the AEMO Gateway Model, the presence of the AEMO raises another option to consider; that is, authentication could also be performed by the AEMO.

The ACCC shared two authentication options with us: either the Data Holder completes the authentication process or the AEMO completes the authentication process (with assistance from, and on behalf of, the Data Holder in relation to the provision of the CDR Consumer's contact details). Authentication under the CDR is performed by the Data Holder or the AEMO requesting identification information for verification purposes and then issuing a One Time Password (**OTP**) to the CDR Consumer.

The scope of the identification information to be requested by the Data Holder or the AEMO (acting on behalf of the Data Holder) is yet to be considered by the ACCC. While collecting as little Personal Information is preferred to avoid the transfer of too much data, sometimes fewer data points prevent identity thieves or fraudsters being caught in their tracks. Since the Data Holder would already have the identity information of the account holder, the risk in collecting the identity information is low (provided the technology supporting the authentication is secure).[51]

The Data Holder will need to consider how much data it requests from the individual before being satisfied that the individual who is making the Consumer Data Request (via the Accredited Person) is the valid account holder. Stakeholders during consultations raised that the identification process needs to align to the stringent requirements under the NECF to avoid duplicating process and maligning procedures. Some Electricity Retailers take the process a step further, by requesting at least 100 points of identification. Whether or not the high watermark approach is adopted, the Data Holder will need to have a clear understanding of when a request is being made under the CDR or not.

Should the individual correctly input the data, an OTP will be issued. The premise of the OTP authentication relies on the Data Holder having the correct contact details so that the unique code can be sent to that individual for verification purposes. From a privacy perspective, if the AEMO performs the authentication process, an additional disclosure of a CDR Consumer's contact information will be shared with a third party. To the extent that the AEMO performing the authentication process minimises repetitive verification by the CDR Consumer, the AEMO may need to store the identification data for some period of time, which presents a risk of data being lost, mishandled, combined or stolen. This would also cause the AEMO to hold customer contact information which could be associated with NMIs. Depending on the branding applied to the identification verification and OTP screens, CDR Consumers may be concerned about how the AEMO collected their contact information for the purposes of authentication.

Views from stakeholders identified both benefits and risks of the Data Holder and the AEMO being directly involved in the authentication process. These included a Data Holder being alerted that a customer was considering moving to another Electricity Retailer, prompting them to offer a better product. However, the downside to this would be more friction with the CDR Consumer engaging in the CDR regime. One stakeholder suggested that there may be more options for authentication, depending on the use cases.

[51] The stakeholders we consulted considered that their existing customer-facing application or portal might facilitate the authentication process (but, this would have to undergo a review and testing).

c. **Consent and authorisation**

As we have described in **Section 7.1(g)** of this report, there are established procedures under the NECF and the VERC to enable consumers of electricity services to access up to two years of data. While these procedures exist, they are underutilised because of issues including low customer engagement, lack of understanding about the meaning of their energy data and the insights that can be drawn from the data, lack of competition to disclose data in a helpful manner and uncertainty about how to use the data in a beneficial way.

The CDR paves the way for third parties to be registered as Accredited Persons by the ACCC to enable these entities to receive CDR Data in a secure manner. Consumers of electricity services will have the option of engaging an Accredited Person to deliver goods or services that will help them to make better decisions in relation to their electricity service. To enable a Consumer Data Request to be processed, the Accredited Person must have received the CDR Consumer's express consent (which can last up to a period of 12 months from the date the consent is validly provided).

Unlike 'explicit informed consent' under the NERL, the scope of the consent provided by the CDR Consumer can be tailored to prescribe what type of data is collected and how that data is collected. Similarly, once valid express consent has been provided, following authentication of the CDR Consumer by the Data Holder or the AEMO, the Data Holder or the AEMO (on the Data Holder's behalf) seeks authorisation to release the CDR Data to the Accredited Person.

Under the CDR Rules, a maximum 12 month consent period is prescribed.[52] Some stakeholders we consulted were comfortable with this restriction (and one stakeholder even suggested that consent should be limited to only a once-off arrangement as it was not clear what the use case would be for any further transfers), whereas others contemplated a longer and more dynamic consent model. However, given most of the stakeholders we consulted are yet to assess the breadth and depth of use cases of the Priority Energy Datasets, it is unclear whether a dynamic and ongoing consent would be feasible. The risk an ongoing consent raises in the energy context is that, while the ADR must explain to the CDR Consumer why it needs further data, the Data Holder may continue to disclose in error data in relation to an account where the account holder has closed the account but where the data flow is linked to the NMI (which stays with the property). Robust technical configurations will need to be considered to avoid, for example, Metering Data being shared with an individual that is no longer related to an Eligible CDR Consumer.

While a robust consent model has been prescribed, one stakeholder commented that a reasonable proportion of its customer base are located in regional areas and they have no digital presence. These 'offline' customers pay their electricity bills in cash at the local post office. Although the focus of the CDR is to encourage digital communications, customers who have never used digital platforms may suffer difficulty and provide consents and authorisations in a limited manner. While there are protections for these consumers in the CDR Rules,[53] further consideration will need to be given to the education and digital literacy enhancements offered to these consumers should they transition 'online'.

The AER pointed to its experience in designing a consent process for its updated platform for EME. It noted that it was important to balance consent so that it is not 'over-explained' and overwhelms the consumer to the point where they cease to engage. The right balance needed to be struck in designing the consent to address privacy risks and a staged approach to explaining the risk. Analysis of consumer use of the updated platform that could be shared may help to provide insights of the consumer experience. It was also anticipated that the CDR consent would help inform and clarify for energy sector participants what good consent looked like.

[52] See rule 4.12(1) of the CDR Rules.
[53] See, generally, subdivision 4.3.2 of the CDR Rules.

Consumers in the energy sector may also be under the age of 18 years. If these individuals are classified as Eligible CDR Consumers, additional safeguards will be required to assess whether or not the consent provided satisfies the requirements in the CDR Rules. The energy-specific CDR rules may need to consider additional obligations on CDR participants to check that a person who is under 18 years old understands the scope of, and consequences of providing, their consent.

The consent and authorisation process prevents Accredited Persons from processing Consumer Data Requests without the knowledge of the CDR Consumer because the CDR Consumer will need to independently authorise the Data Holder or the AEMO via a separate communication channel.

Stakeholder feedback indicated that a further understanding of the potential granularity of the energy datasets would help determine the nature of the consent, as well as the necessary transparency mechanisms. A further understanding of the role of the AEMO would inform the design and the visibility of its role.

d. **The AEMO as a Gateway**

A 'designated gateway' is intended to "facilitate the transfer of CDR data between a Data Holder and an ADR or CDR consumer".[54] The AEMO was identified at an early stage in the development of the CDR framework as an option for a gateway data access model in the energy sector.[55] The ACCC led an extensive stakeholder consultation process on several data access models for CDR data in the energy sector.[56] Following this consultation, the ACCC identified its preference for the AEMO Gateway Model.[57] This was based on the ACCC's model selection criteria, which included security and privacy, user functionality, cost of infrastructure, scalability and interoperability.

The AEMO Gateway Model was preferred because it would allow the AEMO to leverage its existing data transfer infrastructure, data assets and IT and industry expertise to enable the timely and effective implementation of the CDR for the Priority Energy Datasets. A majority of stakeholders who supported this model expressed a view that the model most comprehensively addressed the assessment criteria.

As a Gateway, the AEMO would be subject to the following CDR Privacy Safeguards only:

i. **PS 1** (open and transparent management of CDR data);

ii. **PS 6** (use or disclosure of CDR data by ADRs or designated gateways);

iii. **PS 7** (use or disclosure of CDR data for direct marketing by ADRs or designated gateways); and

iv. **PS 12** (security of CDR data, and destruction or de-identification of redundant CDR data).

The CDR PIA provided an analysis of the APPs and the CDR Privacy Safeguards as they would apply to data flows within the CDR framework.[58] The rules to be developed by the ACCC for the energy CDR may also include provisions relating to the disclosure, collection, use, accuracy, storage, security or deletion of CDR Data by a designated gateway.[59] In addition, the APPs (other than APPs 6, 7, and 11) apply to a designated gateway to the extent that CDR Data is classified as Personal Information.[60]

---

[54] *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, Explanatory Memorandum, paragraph 1.95.
[55] *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, Explanatory Memorandum, paragraph 1.98.
[56] See the ACCC's Consultation Paper on Data Access Models for CDR in Energy, 25 February 2019.
[57] See the ACCC's Consumer Data Right in Energy Position Paper, Data Access Model for Energy Data, 29 August 2019.
[58] See Part F of the CDR PIA.
[59] Section 56BG of the CCA.
[60] Section 56EC(4)(d) of the CCA.

The expertise and resources of the AEMO, given its current energy market roles, including those facilitating and managing data flows can be harnessed to help reduce the likelihood of errors in data flows that could result in a privacy incident or breach. The proposed AEMO Gateway also allows for a unified single source of data management, consent management and accreditation confirmation. This may allow for greater control and monitoring of privacy risks associated with the requirement for informed consent to collect, disclose, hold or use CDR Data. It also helps improve data security through a reduction in data links and authentication processes, which in turn directly addresses and reduces security risks associated with the flow of energy data.

Conversely, this centralised point of access also creates a risk from a security and privacy perspective in that it will potentially provide a single point of failure from access due to being a target for malicious cyber-attacks or as a result of other security breaches. Should the AEMO perform the authentication process, it may become the repository of Personal Information of individuals that it has verified. This could make the AEMO a greater target given the storage of this type of data (in addition to potentially contextualising the data that it can access about NMIs).

The stakeholders consulted noted that the AEMO is not well known by consumers given its role and the introduction of a third party to or through whom CDR Data will be transferred raises an inherent privacy risk. Views were expressed that on the one hand consumers should be educated about the AEMO's role in the energy CDR as the Gateway, but on the other hand it was queried whether consumers needed to know about the AEMO's role at all.

Stakeholders indicated that at this point in time they could not provide informed views about the risks and impacts of the AEMO Gateway Model given the early stages of its development and the need for further consultation to be undertaken to understand the CDR environment it would operate in and the nature of its current privacy practices. It is noted that the AEMO has undertaken and is undertaking extensive consultation and research and is obtaining expert input into the range of privacy, IT, data, security and consumer issues that will be raised by the AEMO Gateway Model and its role and responsibilities. It expressed the strong view that is was important for the features of the energy sectors and the datasets to be well understood and that the consumer should be central to the approach.

7.7 Energy CDR data flows

a. Mapping out the relevant energy data flows helps to identify when and by whom the relevant data is being collected, disclosed, transmitted and shared, and used. The CDR PIA mapped out the data flows based on the design framework, draft CDR Rules, working Consumer Data Standards and the authentication model proposed for the CDR regime's application to Open Banking.[61] Some of the key features of the energy CDR which impact the data flows which are described in this report are:

   i. the inclusion of the Gateway between a Data Holder and an Accredited Person / ADR;

   ii. energy data is connected to a premises and energy consumption may not relate to only the account holder; and

   iii. the different relationships consumers have with energy data, e.g. as an account holder, an occupier of a premises and consumer of electricity.

b. Based on the above and the applicable themes explored in this report, we have mapped the data flows based on the AEMO Gateway Model and the proposed authentication models shared with us by the ACCC. These data flow maps are displayed in **Appendix 2** to this report. Two data flow maps are presented, with a high-level, step-by-step walkthrough of each flow process from start to finish.

[61] See Part G of the CDR PIA.

c. The first data flow map, *Alternative Authentication Model #1*, describes the data flows where the Data Holder performs the authentication process. The second data flow map, *Alternative Authentication Model #2*, describes the data flows where the AEMO Gateway performs the authentication process. We note that these models have been proposed by the ACCC and have not been settled by the ACCC.

Part 8. Analysis of Privacy Impacts and Risks

a. This assessment of privacy impacts and risks supplements the CDR PIA, whose scope considered the establishment of the CDR framework and Open Banking. Since the CDR PIA was finalised, there have been a number of developments in relation to the design and application of the CDR framework in Open Banking and in the energy sector.

b. Having regard to these developments, our assessment considered the information flows mapped in the CDR PIA, **Steps 0 to 10** as set out in Part G of the CDR PIA ("Analysis of Risks Associated with Information Flows in the CDR Regime"). Our analysis of the risk and impacts has focussed in particular on **Step 2** ("ADR obtains technical information from the ACCC's CDR ICT system to send request for CDR Data to the Data Holder") through to **Step 7A** ("ADR uses CDR Data to provide goods or services requested by the CDR Consumer") inclusive, excluding **Step 5** and including **Step 7D**. These steps are most relevant to the data flows in the energy CDR given the designation of the Gateway and the alternative authentication models being considered by the ACCC for the energy CDR.

c. In addition to the risks that were identified in the CDR PIA, we identify the impacts and risks from the energy data flows, existing mitigation strategies and make recommendation to further reduce the particular risk, or where possible, avoid it. This includes the rule making powers in section 56BG of the CCA in relation to designated gateways for various matters such as:

   i. the disclosure, collection, use, accuracy, storage, security or deletion of CDR Data; and

   ii. acting between the CDR Consumer, Accredited Person and Data Holder in relation to the making of a valid Consumer Data Request and subsequent to the disclosure of CDR Data.

8.1 Authentication models

The following table maps the alternate data flows based on the two proposed authentication models.[62] The data flows follow from the Eligible CDR Consumer giving consent to an Accredited Person to collect CDR Data on their behalf for use in providing a good or a service to the CDR Consumer, as described in data flow Step 1B of the CDR PIA. The maps of these data flows are displayed in **Appendix 2** to this report.

Data flow step in the CDR PIA	Open Banking information flow (from the CDR PIA)	Alternative Authentication Model #1 for the energy sector – authentication performed by the Data Holder	Alternative Authentication Model #2 for the energy sector – authentication performed by the Gateway
2	Accredited Person (**AP**) obtains technical information from the ACCC's CDR ICT system to send request for CDR Data to the Data Holder (**DH**).	- AP contacts Gateway seeking access to eligible CDR Consumer's data (in accordance with CDR Consumer's consent). - Gateway contacts ACCC's Register of Accredited Persons to retrieve the authentication details in relation to AP. - Gateway authenticates AP using the data obtained from the Register.[63]	

[62] We note that the two proposed authentication models, as reflected in this report, are subject to consultation and may be amended by the ACCC.
[63] We note that the AEMO Gateway may need to communicate a rejection to the ADR if the authentication fails.

Data flow step in the CDR PIA	Open Banking information flow (from the CDR PIA)	Alternative Authentication Model #1 for the energy sector – authentication performed by the Data Holder	Alternative Authentication Model #2 for the energy sector – authentication performed by the Gateway
3	AP sends a request to DH on behalf of CDR Consumer. AP then redirects the CDR Consumer to DH's system.	- Gateway communicates with the applicable DH about the CDR Consumer's request for CDR Data. - DH sends an OTP to the CDR Consumer.	- Gateway communicates with the applicable DH about the CDR Consumer's request for CDR Data, and requests the CDR Consumer's contact details for the issuance of the OTP. - DH provides the CDR Consumer's contact details to Gateway.[64] - Gateway sends the OTP to the CDR Consumer on behalf of DH.
4	CDR Consumer authorises DH to release their CDR Data to AP.	- CDR Consumer enters the OTP in DH's system. - DH confirms the successful authentication with the CDR Consumer to the Gateway along with information linking the CDR Consumer to the relevant NMI.[65]	- CDR Consumer enters the OTP in Gateway's system.
5	DH confirms that AP is accredited.	- See Step 2 above.	
6	DH transfers CDR Data to AP, and AP collects that CDR Data.	- AP submits a Consumer Data Request for a specific set of CDR Data in accordance with the CDR Consumer's consent. - Consumer Data Request passes through Gateway to DH.[66] - In response to the Consumer Data Request, DH discloses the CDR Data to AP via Gateway.	- Gateway confirms the CDR Consumer's authenticated request and provides the authorised Consumer Data Request to DH.[67] - DH discloses CDR Data to AP via Gateway.
7A	ADR uses CDR Data to provide goods or services requested by the CDR Consumer.	- ADR uses CDR Data to provide the goods or services requested by the CDR Consumer.	

[64] We note that the scope of what will be included as "contact details" is being developed by the ACCC.
[65] We note that the Data Holder may need to communicate a rejection to the CDR Consumer if the authentication fails.
[66] We note that the AEMO Gateway may not pass through the Consumer Data Request to the Data Holder in the instance that the Consumer Data Request relates to data that is held by the AEMO Gateway in its capacity as a Data Holder.
[67] We note that the AEMO Gateway may need to communicate a rejection to the CDR Consumer if the authentication fails. We also note that the AEMO Gateway may not need to pass on the Consumer Data Request to the Data Holder if the Consumer Data Request pertains to CDR Data held by the AEMO Gateway in its capacity as a Data Holder.

8.2 Analysis of privacy risks

***DATA FLOW STEP 1B**: CDR Consumer gives consent to Accredited Person to collect and use their CDR Data*

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
1	Data Holders will have their own processes for different levels of account authorisation. A joint account holder or an authorised representative on the account makes a request beyond their authority. The Data Holder may disclose CDR Data to the authorised representative who had no relevant authority from the primary account holder to make such a request.	Although a joint account holder or an authorised representative could approach an Accredited Person to make a Consumer Data Request, their personal details will be verified once the Gateway communicates their details to the Data Holder for the purpose of authentication. Part 4 of Schedule 3 to the CDR Rules provides guidance for Consumer Data Requests relating to joint accounts in Open Banking and for Data Holders to provide a joint account management service.	There are currently no rules in the CDR Rules which address 'authorised representatives'. If authorised representatives are to be eligible to access CDR data, we recommend that rules be considered that address this issue. The Data Holder should be responsible for conducting checks against its databases to assess the authority granted to the authorised representative, and to proceed on that basis. If the authorised representative does not have the authority to request CDR Data or retrieve data in relation to the account, the Data Holder should not be able to authenticate the authorised representative, and the Data Holder should refuse to disclose CDR Data to the Accredited Person via the Gateway. Rules similar to Part 4 of Schedule 3 of the CDR Rules should be made for joint account holders and authorised representatives, subject to specific consultation. See **Recommendation 3**.
2	An individual under 18 years of age makes a Consumer Data Request to an Accredited Person. Through stakeholder consultations, we understand that there may be a small number of individuals under 18 years of age that hold electricity accounts. The individual aged under 18 years of age may lack the capacity to consent in accordance with the CDR Rules.	Should the ACCC extend the scope of the Eligible CDR Consumer in the energy sector to include an individual under the age of 18 years, the OAIC's APP Guidelines provide for its approach to seeking consent from individuals under 18 years of age and the capacity of such individuals to make informed consent, and any assumptions that can be made in relation to individuals over the age of 15 years.	Currently the CDR Rules only contemplate an individual who is over 18 years of age qualifying as an Eligible CDR Consumer. We recommend that the ACCC consider whether individuals under the age of 18 years should not be included in the CDR regime, and that, if so, specific rules be developed to require Accredited Persons to assess whether or not the consent provided by the CDR Consumer satisfies the requirements in the CDR Rules. The Data Holder

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
			must also be required to consider the age of the CDR Consumer as part of the authentication process. The CX Standards being developed by the Data Standards Body will also need to reflect a different experience for individuals under 18 years of age. See **Recommendation 3**.
3	The CDR Consumer requests access to data in relation to a closed or inactive account. An Accredited Person may need this historical data to provide an effective good or a service to a CDR Consumer. However, this CDR Data may contain information about a different individual who previously held an account in relation to the NMI.	As described above, only an Eligible CDR Consumer can make a Consumer Data Request to a Data Holder. The current approach in Open Banking limits an Eligible CDR Consumer to an individual who has an open account with a Data Holder. CDR Privacy Safeguard 4 requires Accredited Persons to take steps to deal with unsolicited CDR Data if it did not seek to collect all the historical data where it did not relate to the Eligible CDR Consumer.	Should the ACCC extend the scope of the Eligible CDR Consumer in the energy sector to include an individual who has an account with a Data Holder that is closed or inactive at the time of the Consumer Data Request, additional controls will need to be developed to ensure the individual is appropriately identified and their request relates to an inactive or closed account that they held for a specific period of time. In addition, CDR Rule 4.26 will need to ensure that an authorisation to a Data Holder does not lapse when the CDR Consumer's electricity account closes if the definition of Eligible CDR Consumer is changed to include closed or inactive accounts in the energy sector and the CDR Consumer has provided consent in relation to this Consumer Data Request. We recommend that as part of the authentication process, the Data Holder must verify that the request is from an Eligible CDR Consumer in relation to that data (whether relating to a current account or if extended, to a closed/inactive account). This will require an additional step so that only the data that relates to when the Eligible CDR Consumer held

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
			the account is transferred, and not all data in relation to the NMI. The CDR Privacy Safeguard Guidelines should be updated to support the effect of such a rule change in relation to an Eligible CDR Consumer, and the authentication and authorisation processes Data Holders must follow. See **Recommendation 3**.
4	The CDR Consumer who makes a Consumer Data Request may be unaware that the data they consented to the Accredited Person collecting will include data disclosed by the Data Holder (pursuant to the consent) that relates to their personal circumstances and what they consider to be sensitive information. CDR Consumers may not wish for information, for example, about their financial Hardship or Concession information to be shared for the purposes of the product or service the Accredited Person is intending to provide them. The collection and use of such information may be relevant to and reasonably necessary for the purpose of providing the product or service that an Accredited Recipient has been requested by the CDR Consumer to provide, and as an ADR it would be authorised to do so by CDR Privacy Safeguard 6 and CDR Rule 7.5(1). Neither CDR Privacy Safeguard 3 (and the CDR Privacy Safeguard Guidelines), nor the CDR Rules, distinguish any CDR Data as sensitive.	Stakeholder feedback suggests that the Billing Data would not specifically reveal whether a person has a Concession or is on a Hardship arrangement (unless this data, which may be included in a CDR Consumer's electricity bill, was directly and voluntarily disclosed to the Accredited Person by the CDR Consumer). However, Billing Data comprises multiple data points including the date of bills issued, the frequency, and the amount of payments and deferred payments (including measures put in place in relation to a customer experiencing Hardship or entitled to a Concession). Together, this data may reasonably indicate to an ADR that a CDR Consumer has a Hardship arrangement or receives a Concession. Metering Data is not available in real time data, which reduces the risk of identifying when a particular person is currently occupying the premises. Also, most properties have appliances and devices that consume electricity even when there are no occupants at the property. CDR Rule 4.11 requires the Accredited Person to clearly indicate to the CDR Consumer which of the particular types of CDR data they are consenting to	Consideration should be given to whether the Consumer Data Standards could prescribe any additional circumstances to address this risk. These standards will assist to enhance the level of transparency provided to CDR Consumers about the types of data being shared. The CX Standards and CX Guidelines should ensure Accredited Persons help CDR Consumers to clearly understand and decide whether they wish to select these specific types of CDR Data relating to their account to share and consideration should be given to how the data clusters are structured so that this can happen. This will support informed consent and avoid CDR Consumers being unaware that the Accredited Person has collected unnecessary information. Rule 3.5 should be reviewed in consultation with Electricity Retailers to understand whether it needs to cover broader potential harms to allow for more flexibility in its application by Data Holders. For example, whether paragraph 3.5(1)(a) of the CDR Rules could be expanded to include a flexible definition of harm.

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
		the Accredited Person making a request to collect. Accredited Persons are also required to comply with CDR Privacy Safeguard 3 in relation to collecting CDR data from Data Holders. The Accredited Person will only be able to make a clear representation about what data they are requesting if they know exactly what types of CDR data they will be receiving from the Data Holder. Data Holders are required to share information about the types of CDR Data for which the Data Holder is seeking an authorisation from the CDR Consumer to disclose (CDR Rule 4.23(c)). Given both the Accredited Person and the Data Holder will have Consumer Dashboards showing CDR Consumers their consent and authorisation, this should help make it clear to CDR Consumers what types of information will be included in the CDR Data that will be collected by the Accredited Person. CDR Rule 3.5 of the CDR Rules permits a Data Holder to refuse to disclose CDR Data in response to a Consumer Data Request if it considers it necessary to prevent physical harm or financial abuse or in any circumstances set out in the Consumer Data Standards. Hardship data or other similar data that may be sensitive to an individual is not unique to the energy sector. The Data Minimisation Principle that underpins the CDR regime requires an Accredited Person to only collect and use CDR data in order to provide goods or services in accordance with a Consumer Data Request.	See **Recommendation 7**.
5	The CDR Consumer's consent does not expire when a property-	CDR Rule 4.14 limits the duration of consent to not exceed 12 months from the time the	We recommend that a trigger to terminate the authorisation is included under CDR Rule 4.26, as

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
	related event occurs (e.g. the sale of property). A trigger in the Data Holder's system does not instruct the system processing the Consumer Data Request to stop when the CDR Consumer is no longer an Eligible CDR Consumer. The consent may not expire at this time and may continue to allow an ADR to collect CDR Data that contains the Personal Information of a third party (e.g. the new owner or occupier of the property).	consent has been validly provided to the Accredited Person. This consent will expire if the CDR Consumer withdraws their authorisation to the Data Holder to disclose the CDR Data in relation to the account in accordance with CDR Rule 4.25(1). However, if the CDR Consumer no longer continues to be an Eligible CDR Consumer in relation to the Data Holder (e.g. because the electricity account has closed within a 12 month period due to the account holder selling the property), this may not then trigger the expiry of the consent (i.e. CDR Rule 4.14(1)).	well as a termination of the consent under CDR Rule 4.14 to ensure that the Data Holder does not continue to disclose, and the ADR does not continue to collect, data that may identify a third party.[68] Consideration should also be given to whether the Consumer Data Standards could set out circumstances in relation to property events where a Data Holder may refuse to continue to disclose CDR data as provided for in CDR Rule 4.7. See **Recommendation 3**.
6	The Accredited Person uses the CDR Data it collects to identify, compile insights in relation to or build a profile of a person who is identifiable and who is not the CDR Consumer who made the Consumer Data Request. For example, a landlord, owners' corporation / body corporate or employer who is the account holder may, through receiving a service from an ADR, receive a profile of the occupants (e.g. tenants, strata owners or employees) of the property. We note that this is a present risk because under the existing data access regime under the NERL account holders can access meter consumption data for up to two years.	Metering Data is not available in real time, which reduces the risk of identifying a particular individual. CDR Rule 4.12(3)(b) prohibits Accredited Persons from seeking consent from CDR Consumers to use or disclose their CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to an identifiable person who is not the CDR Consumer who made the Consumer Data Request. Stakeholder consultation suggests that it is unclear how effective this rule will be on an Accredited Person and whether it will limit their ability to use the CDR Data. There was also uncertainty expressed by stakeholders about whether it is in fact possible to identify or reasonably identify an individual who is not the CDR Consumer from the CDR Data that is collected by the Accredited	Through further testing and consultation on specific use cases, the application of CDR Rule 4.12(3)(b) may need to be reconsidered for the energy CDR if it is found that compiling insights or building a profile about a non-CDR Consumer (who is identifiable) is inevitable and when the scope of the Priority Energy Datasets is expanded in the future. The ACCC should consider rules that strike an appropriate balance between the privacy rights of the CDR Consumer and any non-CDR Consumer (who will most likely be known to the CDR Consumer). See **Recommendation 3**.

[68] We acknowledge that the ACCC submitted a submission to the AEMO on 27 March 2020 in response to a consultation, *MSATS Standing data review*. A recommendation was made by the ACCC in relation to when a NMI has changed customer.

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
		Person based on the Priority Energy Datasets.	

***DATA FLOW STEP 2**: ADR obtains technical information from the ACCC's CDR ICT system to send request for CDR Data to the Data Holder*

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
1	The Accredited Person discloses unnecessary Personal Information relating to the CDR Consumer to the Gateway.	There are currently no provisions in the CDR Rules to address this risk as no rules have yet been made for a designated gateway.	The CDR Rules should expressly prescribe what Personal Information relating to the CDR Consumer (if any) needs to be disclosed to the Gateway for the purposes of processing the Consumer Data Request. The CDR Rules will need to consider the options for the authentication model to require the Accredited Person to share the minimum Personal Information as possible. See **Recommendation 3**.
2	The pathway between the Accredited Person and the Gateway is compromised. The data disclosed by the Accredited Person could be intercepted by a third party and used for malicious purposes, or transformed to change the identity of the CDR Consumer making the Consumer Data Request.	The Data Standards Body is responsible for drafting the Consumer Data Standards which include technical API and information security profile standards.	Following the commencement of the Designation Instrument for the energy CDR, we recommend the Data Standards Body consider the additional API and information security profile requirements to accommodate the AEMO Gateway Model in consultation with the AEMO and relevant stakeholders. See **Recommendation 2**.
3	The Gateway refuses to authenticate the Accredited Person. The Gateway may for example independently have identified a risk in relation to the Accredited Person because it is aware of or has information in relation to other matters that might not be reflected in the Register of Accredited Persons.	While a Data Holder is able to refuse to disclose the required CDR Data in response to a Consumer Data Request to prevent physical or financial harm or because it might impact the security of the Register of Accredited Persons or the Data Holder's systems (see CDR Rule 4.7(1)), an equivalent right for the Gateway does not exist.	We recommend that the role of the Gateway will perform in relation to verifying the Accredited Person against the Register of Accredited Persons should be considered in light of the potential risks and whether it should be granted a discretion to refuse to authenticate the Accredited Person, where there is a reasonable belief of harm to the CDR infrastructure or an individual. See **Recommendation 3**.

***DATA FLOW STEP 3**: ADR sends a request to the Data Holder on behalf of the CDR Consumer. ADR then redirects the CDR Consumer to the Data Holder's system.*

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
1	The pathway between the Gateway and the Data Holder is compromised. The data disclosed by the Gateway could be intercepted by a third party and used for malicious purposes, or transformed to change the identity of the CDR Consumer making the Consumer Data Request.	The Data Standards Body is responsible for drafting the Consumer Data Standards which include technical API and information security profile standards.	Following the finalisation of the Designation Instrument for the CDR regime to apply to the energy sector, we recommend the Data Standards Body consider the additional API and information security profile requirements to accommodate the AEMO Gateway Model. See **Recommendation 2**.
2	The Data Holder discloses incorrect Personal Information of the CDR Consumer to the Gateway. If the Gateway performs the function of authenticating the CDR Consumer, it will need to receive accurate, complete and up-to-date Personal Information to enable the correct CDR Consumer to be contacted. To enable the Gateway to contact the correct CDR Consumer, an additional disclosure of Personal Information from the Data Holder to the Gateway will need to occur.	The Gateway does not know who the CDR Consumers are as it does not hold a list of individuals (including their contact details) associated with a NMI or Electricity Meter Number as the primary account holder.[69] There are currently no rules in the CDR Rules on this subject matter. The Personal Information of the CDR Consumer disclosed by the Accredited Person to the Gateway and then shared with the Data Holder should in any event align to the Data Holder's database. If it does not align, then this could be because the CDR Consumer is not an Eligible CDR Consumer in relation to the account, the verifying data held by the Data Holder is not consistent or up-to-date, or the request may not be an eligible Consumer Data Request and the Data Holder or Gateway will not issue an OTP. Only following a successful verification will the Data Holder disclose relevant Personal Information of that CDR Consumer to the Gateway for the purposes of authentication.	Under Data Flow Step 2, depending on what Personal Information of the CDR Consumer is disclosed by the Accredited Person to the Gateway (if any), the Data Holder should only supplement that data to enable the Gateway to correctly contact the CDR Consumer for the purpose of authentication. If the data is incorrect and through the authentication process this is identified, we recommend that the Gateway be required to notify the Data Holder so that this can be rectified (e.g. update customer database and systems). See **Recommendation 3**.

[69] We note, however, if the Gateway performs the authentication function, it may develop a database of previously verified individuals. In these circumstances, it may have the contact details of repeat CDR Consumers, but the data held may not be up-to-date. It will need to be considered how this data is maintained from a data quality perspective.

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
3	The Data Holder discloses insufficient or unnecessary Personal Information of the CDR Consumer to the Gateway for the purposes of the authentication.	There are currently no rules in the CDR Rules to address this risk.	The CDR Rules should expressly prescribe what Personal Information of the CDR Consumer needs to be disclosed by the Data Holder to the Gateway for the purposes of authentication (should the Gateway conduct the authentication). See **Recommendation 3**.
4	A third party (outsourced service provider to the Gateway or the Data Holder) performs the authentication process. While the responsibility to comply with the CDR regime lies with the Gateway or the Data Holder, an additional flow of data to a third party service provider may compromise the privacy and security of a CDR Consumer's Personal Information.	There are currently no rules in the CDR Rules to address this risk. The ACCC is currently engaged in consultation in relation to intermediaries and is yet to deliver its position on this subject matter.	The ACCC should consider rules which require that any disclosure of Personal Information by the Gateway and/or the Data Holder during authentication is properly managed via an appropriate outsourcing arrangement. See **Recommendation 3**.
5	The CDR Consumer is not properly identified for authentication purposes depending on the type of CDR Data is the subject of the Consumer Data Request.	There are currently no rules in the CDR Rules on this subject matter. Through stakeholder consultations, the Electricity Retailers confirmed that they have stringent authentication procedures which are standard. The 'authentication flows' in the Consumer Data Standards prescribe that "Data Holders must request a user identifier that can uniquely identify the customer and that is already known by the customer in the redirected page". Different processes undertaken by Data Holders will influence the extent of how much identity information is requested from the CDR Consumer for authentication.	The amount and type of identity information will need to be balanced with the object of the CDR, promoting accessibility, and being consistent with the approach across all sectors to which the CDR applies. We do not believe that specific rules should be prescribed, however the CDR participant performing the authentication needs to be mindful of ensuring that they are dealing with the correct CDR Consumer (i.e. a valid account holder). See **Recommendation 3**.

***DATA FLOW STEP 4**: CDR Consumer authorises the Data Holder to release their CDR Data to the ADR*

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
1	The AEMO is able to associate the identities of people to NMIs that is holds in its database. Once the Accredited Person submits the Consumer Data Request to the AEMO, the AEMO will need to unpack this dataset to understand which Data Holder to approach. Following the successful authentication of the CDR Consumer pursuant to Alternative Authentication Model #1, the CDR Consumer's NMI will be shared with the AEMO. If the AEMO does not have appropriate database controls, including authorised access permissions and segregated databases at a minimum, the AEMO will be able to associate the identity of a person to a NMI. This will change the level of sensitivity of the NMI Standing Data held by the AEMO, if databases are not appropriately quarantined and separated.	There are currently no rules in the CDR Rules to address this risk.	The AEMO will collect information about the CDR Consumer from the Accredited Person and the Data Holder which will cause it to have enough information to associate the identity of a person to a NMI. To the extent that the AEMO is required to retain the data collected from the Accredited Person for the purpose of processing the Consumer Data Request, such data will need to be kept separate from the database storing NMI Standing Data. Otherwise, the AEMO will hold enough data for a NMI to be associated with an individual, which will change the sensitivity of the data held by the AEMO. See **Recommendation 2**.
2	The NMI or Electricity Meter Number disclosed by the Data Holder to the Gateway is incorrect when the Gateway needs to send particular datasets to the Accredited Person in response to the Consumer Data Request. For example, NMI Standing Data belonging to an account not held by the CDR Consumer is disclosed to the Accredited Person which may reveal the identity of a non-CDR Consumer. In addition, the correct NMI might have been shared by the Data Holder however the registration	There are currently no rules in the CDR Rules to address this risk.	The ACCC should consider whether the Accredited Person should be required to collect any information that is necessary to ensure that the Gateway and Data Holder can appropriately source the CDR Consumer's data (If any). This will enable the Data Holder to verify (prior to the authentication of the CDR Consumer) that, for example, the CDR Consumer's NMI matches the NMI registered to the account the CDR Consumer holds. This will ensure that even if the Data Holder discloses the incorrect NMI to the Gateway, the Gateway can identify this

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
	of the NMI in the MSATS database has errors.		error (i.e. that the NMIs do not match) with the Data Holder prior to the disclosure of CDR Data that it holds to the Accredited Person. If there is a mismatch, this will allow the Accredited Person to check with the CDR Consumer to ensure that the correct NMI has been supplied before any data is disclosed by the Data Holder. See **Recommendation 3**.

***DATA FLOW STEP 6**: Data Holder transfers the CDR Data to the ADR; and ADR collects that CDR Data*

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
1	Stakeholder feedback confirmed that it is a recognised issue in the energy sector that the MSATS database contains errors due to incorrect registrations, human error, street naming convention, subdivisions and other matters. The CDR Consumer specifies a NMI, Electricity Meter Number or property address to the Accredited Person but the registration of the NMI in the MSATS database is incorrect. NMI Standing Data retrieved in connection with a NMI is disclosed to the Accredited Person that is linked to an account that is not related to the CDR Consumer.	Stakeholder feedback suggest there are piecemeal steps to address this issue.	Treasury, the ACCC and the Data Standards Body should undertake further consultation with energy stakeholders, including the AER, the AEMO and the Electricity Retailers, to understand how the existing energy regulatory framework needs to adapt to remedy this issue to mitigate the continued risk of NMI Standing Data and Metering Data being disclosed to the Accredited Person about an individual that is not the CDR Consumer or an associate of the CDR Consumer. See **Recommendation 6**.
2	The CDR Data collected by the Gateway from the Data Holder is different to the CDR Data that is disclosed by the Gateway to the Accredited Person as a result of the CDR Data being transformed into a different format where the substance of the datasets have changed.	There are currently no rules in the CDR Rules to address this risk.	The scope and features of the Gateway's role as a designated gateway needs to be clearly described in the CDR Rules. From a privacy perspective, as a data access model and given the reasons why the ACCC preferred this model, where the Gateway does not act in the capacity of a Data Holder, it should only transmit the CDR Data from the

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
			Data Holder to the Accredited Person. Section 56BG(3)) of the CCA restricts the AEMO to acts related to the gateway role it is designated. Permitted access or use of CDR Data that is transmits from Data Holders in response to an authenticated Consumer Data Request should be limited to supporting the transmission of the data (such as collating information from multiple Data Holders into a single payload for an ADR). It should not be permitted to otherwise collect and hold, transform, access, copy, delete or overwrite the CDR Data. See **Recommendation 2**.
3	The Gateway discloses data to the Accredited Person that is not linked to the NMI, Electricity Meter Number or the property address of the CDR Consumer as disclosed by the Data Holder. This may arise because of a human error or a technical deficiency in the Gateway's system.	The Consumer Data Standards provide technical API standards to ensure that minimal human involvement occurs through the data flow process.	The Consumer Data Standards should support the digitally enabled transmission of the relevant datasets from the Gateway (which independently matches the data disclosed by the Accredited Person to the Gateway about the CDR Consumer) so that data errors are minimised. See **Recommendation 2**.
4	The Gateway shares NMI Standing Data or Metering Data that contains data before the time the CDR Consumer held the account in relation to the NMI, or acquired or occupied the property. The Data Holder does not disclose to the Gateway the date when the CDR Consumer commenced holding the account with the Data Holder.	After a CDR Consumer gives consent to the Accredited Person and authorises the Data Holder to disclose CDR Data, there is currently no rule in the CDR Rules which requires the Data Holder to disclose to the Gateway the date the CDR Consumer commenced holding the account with the Data Holder.[70]	Provided that the Data Holder has verified the Eligible CDR Consumer, the Gateway will need to know this type of account information about the CDR Consumer so that it does not share data from the NMI Standing Data fields or the Metering Data sets that might contain information that identifies or reasonably identifies an individual who is not the CDR Consumer. See **Recommendation 3**.

[70] We acknowledge that the ACCC submitted a submission to the AEMO on 27 March 2020 in response to a consultation, *MSATS Standing data review*. A recommendation was made by the ACCC in relation to when a NMI has changed customer.

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
5	The CDR Data transmitted or held by the Gateway is compromised.	The AEMO has been identified by the ACCC as the preferred data access model for energy CDR because of factors including data security. The AEMO has developed information security control, privacy controls and system protection controls to ensure that its technological infrastructure is not easily compromised. Routine internal audits of its systems take place with maturity assessments performed to identify gaps and improvement opportunities for remediation and enhancement. From stakeholder consultations, we understand that the AEMO assesses its operations against the Australian Energy Sector Cyber Security Framework.	A separate PIA (including an information security assessment) on the operation of the designated gateway for the energy CDR regime should be conducted in consultation with the OAIC, the Data Standards Body and the ACCC to assess the risks associated with the design, systems, infrastructure and purpose of the Gateway. This will help guide the development of additional CDR Privacy Safeguard, Consumer Data Standards, CX Standards and energy rules to address identified risks including in relation to the disclosure, collection, use, accuracy, storage, security or deletion of CDR Data for which there are CDR Consumers in its role acting between the various CDR participants. In addition, the level of effort required for the Gateway's system to function under the CDR will need to be reviewed to ensure that it can cope with the demand and increased API calls. See **Recommendation 2**.
6	Information disclosed by the Data Holder of DER Data includes the Personal Information of a third party (e.g. the installer of the DER or the individual who has purchased the DER on behalf of the CDR Consumer).	At present, there are no rules in the CDR Rules imposing obligations on the Data Holder to cleanse the DER Data prior to disclosing them to the Accredited Person via the Gateway. Clause 3.7E(h)(2) of the NER requires the AEMO to consider the risks of including data in the DER Register against confidentiality and privacy.	Depending on the scope of the DER Data, we recommend that prior to disclosing this CDR Data in response to a Consumer Data Request, the Data Holder (i.e. the AEMO) should be required to remove information about third parties from the relevant datasets. See **Recommendation 3**.

***DATA FLOW STEP 7A**: ADR uses CDR Data to provide goods or services requested by the CDR Consumer*

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
1	In the interests of the interoperability of the CDR regime in the Australian economy, the CDR Consumer instructs an ADR to port their CDR Data to a third party (which could be an Accredited Person) in machine-readable form. The transmission of this data is compromised or the ADR manipulates the data prior to disclosing it to the third party.	The ACCC has been consulting on the inclusion of intermediaries in the CDR regime across all sectors.	We recommend specific rules are developed to regulate the disclosure of CDR Data by ADRs to a third party in machine-readable form. See **Recommendation 3**.

***DATA FLOW STEP 7D**: ADR de-identifies CDR Data and discloses the de-identified data to third parties*

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
1	The security of the Gateway and the systems which interface it will be critical to the functioning and integrity of and trust in the energy CDR.	The security, the deletion of redundant data and requirements for when and how CDR Data must be de-identified and when de-identified CDR Data may be used, are set out in CDR Privacy Safeguard 12, the CDR Rules and the Consumer Data Standards. The CDR Privacy Safeguard Guidelines further address the requirements of CDR Privacy Safeguard 12, which applies to ADRs and designated gateways, which will include the AEMO, but not to Data Holders (to whom APP 12 will apply). The CDR Privacy Safeguard Guidelines explain the requirements in CDR Privacy Safeguard 12 for the secure transfer of CDR Data between Data Holders and ADR, the steps that ADRs should take to manage information security, the information security capability they must maintain, the formal controls program they must implement and the detection and management of information security incidents, including compliance with the 'notifiable data breaches scheme' under the	These requirements and steps will need to be met in building and designing the Gateway platform and CDR environment for the Gateway. The scope of this SPIA and the current early stages of the development of the Gateway do not allow this report to consider security issues in detail. However, the CDR Rules and CDR Privacy Safeguard Guidelines should be updated to address security issues identified in further development of and consultation on the Gateway and any PIA that is undertaken in relation to it. A separate set of information security guidelines for the platform and how it interacts with ADRs and Data Holders should also be developed having regard to the current arrangements the AEMO has in place for protecting energy data flows as the market operator. See **Recommendation 2**.

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
		Privacy Act. The CDR Privacy Safeguard Guidelines refer further to the ACCC's Supplementary Accreditation Guidelines on Information Security.	

Part 9. Other Privacy Risks, Issues and Considerations

From our stakeholder consultations and review of materials in the context of the energy regulatory framework, proposed authentication models and the proposed role of the Gateway, we have identified other issues for consideration to include in this report which are relevant to the impact of the development of the energy CDR. The considerations are not intended to be exhaustive, the order is not suggestive of any priority and they do not necessarily focus on privacy-related issues. However, given the current status of the proposed Designation Instrument, feedback on the progress of stakeholder understanding about how the AEMO Gateway Model will operate and the scope of the Priority Energy Datasets, we believe the following considerations may be of assistance to the development of the energy CDR and assist with further consultations.

9.1 Balancing existing regulatory requirements with competing CDR requirements

As we have described in this report, the energy sector is a regulated industry. The current regulatory environment prescribes rules in relation to the handling and treatment of energy data. We have not undertaken a detailed assessment in this report about the data retention obligations on participants in the energy sector, particularly the AEMO and Electricity Retailers.

9.2 Definitions of key energy CDR concepts and terms

The current CDR Rules, CDR Privacy Safeguard Guidelines and the CX Standards and CX Guidelines were developed with Open Banking as the objective. These foundational instruments will need to be developed for the energy CDR to support the clear definition and understanding of key concepts in the energy CDR, for example the definitions and descriptions of what is included in a Consumer Data Request for information relating to an electricity account. The Data Minimisation Principle must be considered and reflected within descriptions and definitions that guide which CDR Data is associated with a customer, and in turn, what information will be collected and used by an Accredited Person.

9.3 Energy consumers currently excluded from CDR

There is the potential for certain individuals who use, consume or pay for electricity services to be unable to participate in the energy CDR. For example, these individuals include a consumer who is not known to the Energy Retailer, those who only have offline accounts and receive paper bills and those from vulnerable groups who have limited understanding of their electricity service. Since the provision of electricity is an essential service, consumers should be equipped with the mechanisms and information to find a better plan for their circumstances and seek an affordable arrangement. An understanding of the benefits of the energy CDR through education and awareness campaigns may encourage these types of individuals with low engagement and energy literacy to set up digital accounts. It is noted that the ACCC is considering future use cases and the inclusion of other energy datasets that would expand the types of consumer groups.

9.4 Dispute resolution

a. Complaints in relation to energy are handled by each of the State and Territory Energy and Water Ombudsman schemes. Electricity Retailers are required to be registered with an ombudsman scheme. Electricity Retailers are also required to have an internal dispute resolution process. They are able to give a very helpful perspective on consumer experience given their roles dealing with complaints from anyone who may be affected by the conduct of an Electricity Retailer.

b. Any consideration of existing sector based dispute resolution schemes will need to have regard to its geographical reach as well as how the scheme may be extended to apply to all energy CDR participants (particularly the AEMO, who may not otherwise be subject to the scheme). It will need to be considered whether the AEMO, having both government and industry shareholders, is able to be a member of an industry scheme, or whether an alternative dispute resolution mechanism would be an appropriate alternative.

c. As CDR Data begins to move between sectors of the economy (for example, from an Electricity Retailer to a fintech entity), it may become difficult for CDR Consumers to know where they should make a complaint (e.g. to an energy External Dispute Resolution (**EDR**) scheme or a banking EDR scheme). Consideration may need to be given to ensuring that complaints can be readily directed to the appropriate scheme, as necessary.

9.5 Use cases for energy CDR Data

Through our research and consultations, we identified that common use cases being considered in the energy industry included: switching plans and tariffs, purchasing solar panels (and understanding feed-in arrangements), purchasing batteries, conducting energy efficient audits and assisting with energy rating assessments for buildings. Use cases with Open Banking included short-term financing for DERs, budgeting for energy costs based on seasonal factors and cash flow management for paying bills. Some stakeholders queried that not all use cases require an ongoing consent (up to 12 months) for CDR Data; a one-time use to collect CDR Data may be sufficient and it should be deleted after the ADR has provided that good or service to the CDR Consumer.

9.6 Exempt energy sellers

a. We note that an 'exempt seller' (e.g. an individual or a body corporate)[71] is not considered to be a Data Holder for the purposes of the CDR because they do not hold a licence or authorisation to operate as an Electricity Retailer. Exempt sellers arise in scenarios where the entity plans to sell electricity incidentally to their main business, as a community service at no cost, and to a defined group of customers at one site (e.g. in the context of an Embedded Network). Exempt sellers must comply with a range of consumer protections under the NERL.

b. When the exempt seller on-charges the supply and usage of the electricity service to the entities that have received the service, they will rely on consumption data for the purpose of apportioning costs. While this process is regulated under the NERL, the consumer protections under the CDR Rules do not apply.

[71] See the AER's webpage "Retailer exemptions", retrieved 4 May 2020.

9.7 Size and capability of Electricity Retailers

The AER noted that there are differing sizes, capabilities and sophistication of Electricity Retailers emerging in the energy sector. This is because there are lower barriers to entry and it was likely that there is a range of awareness and understanding about compliance in a system which does not have as many checks and balances as Open Banking. Some Electricity Retailers will not have the ability to invest in technology or resourcing to prepare for the energy CDR and will need more time. Therefore, a phased approach may be more appropriate.

Appendix 1: Glossary and Abbreviations

A. Glossary

Accreditation Registrar means the person appointed under subsection 56CK(1) of the CCA. At present, this person is the ACCC.

Accredited Data Recipient has the meaning given to that term in section 56AK of the CCA.

Accredited Person means a person who holds an accreditation by the Data Recipient Accreditor (i.e. the ACCC) under subsection 56CA(1) of the CCA. This person and the ADR are the same person.

Australian Energy Market Operator means the person who operates and manages the NEM and who will likely take the role of providing the Gateway for CDR Data for the energy CDR.

AEMO Gateway Model means a data access model described in the ACCC's *Position Paper (Data Access Model for Energy Data)* dated August 2019.

ACCC means the Australian Competition and Consumer Commission who has CDR rule making powers and is responsible for, among other things, maintaining the Register of Accredited Person for the purpose of the CDR regime as set out in Part IVD of the CCA.

Australian Consumer Law means Schedule 2 to the CCA.

Australian Information Commissioner means the individual appointed as such by the OAIC.

Australian Privacy Principles means the Australian Privacy Principles in Schedule 1 to the Privacy Act.

Average Daily Load means an electricity consumer's average daily consumption of electricity measured in kWhs.

Billing Data means historical billing information for each connection point to which electricity is delivered in the NEM including records of bills issued, payments received and payment arrangements. This type of data has been identified as a Priority Energy Dataset.

CCA means the *Competition and Consumer Act 2010* (Cth).

CDR Consumer has the meaning given to that term in subsection 56AI(3) of the CCA.

CDR Data has the meaning given to that term in subsection 56AI(1) of the CCA.

CDR Participant has the meaning given to that term in subsection 56AL(1) of the CCA.

CDR Privacy Safeguards means the 13 privacy safeguards set out in Division 5 of Part IVD of the CCA for which the OAIC is responsible for administering.

CDR Privacy Safeguard Guidelines means the version 1.0 guidelines issued by the OAIC in February 2020 in relation to how it will interpret and apply the Privacy Safeguards when exercising its functions and powers relating to them under Part IVD of the CCA.

CDR Rules means the Competition and Consumer (Consumer Data Right) Rules 2020 made by the ACCC dated 4 February 2020.

Clean Energy Regulator means the independent statutory authority of the Commonwealth responsible for administering schemes to assist with the measurement, management, reduction and offset of Australia's carbon emissions.

Concession means a discount or rebate on the customer's bill because the customer is eligible for a government funded energy charge rebate, concession or relief scheme.

Consumer Dashboard means:

a) in relation to an Accredited Person, an online service described in paragraph 1.14(1) of the CDR Rules; and
b) in relation to a Data Holder, an online service described in rule 1.13(1)(a) of the CDR Rules.

Consumer Data Request means a request for CDR Data as described in rule 1.4 of the CDR Rules.

Consumer Data Standards means the technical standards developed by the Data Standards Body which represent the current baseline for implementation of the CDR by the relevant participants.

Consumer Experience Guidelines means the consumer experience guidelines developed by the Data Standards Body to support the implementation of the CX Standards. See version 1.3.0, 17 April 2020.

Consumer Experience Standards means standards developed by the Data Standards Body in relation to consumer experience under rule 8.11 of the CDR Rules and may have binding effect under section 56FA of the CCA. See version 1.3.0, 17 April 2020.

Customer Provided Data means data provided by the CDR Consumer including name of account holder, contact details including billing address or postal address, and information provided about the property including appliances. This type of data has been identified as a Priority Energy Dataset.

Data Holder has the meaning given to that term in section 56AJ of the CCA.

Data Minimisation Principle means a requirement that needs to be complied with by an Accredited Person and has the meaning given to that term in rule 1.8 of the CDR Rules.

Data Standards Body means a person appointed under section 56FJ of the CCA. At present, this person is CSIRO's Data61.

Data Recipient Accreditor means the person appointed under subsection 56CG(1) of the CCA. At present, this is the ACCC.

Derived CDR Data has the meaning described in subsection 56AI(2) of the CCA.

Designation Instrument means a statutory instrument designating a particular sector to implement the CDR regime.

Distributed Energy Resource means a consumer-owned device that, as an individual unit, can generate or store electricity or have technological capability to actively manage energy demand.

DER Data means data about DERs (e.g. details on batteries and panel installations). This type of data has been identified as a Priority Energy Dataset.

DER Register means a database of information about DER devices that is managed by the AEMO. The register officially launched on 1 March 2020.

Electricity Distributor means a person which owns and maintains the distribution networks, including electricity power lines and power poles that carry electricity to properties and infrastructure.

Electricity Meter Number means a unique identifier for an electricity meter that is different to the NMI, and changes when a new meter is installed.

Electricity Retailer means an entity that has been granted a retailer authorisation or license for the selling of electricity to a person for premises by a governing body (e.g. the AER or ESC who provide the authorisation or licence).

Eligible CDR Consumer means a CDR Consumer that is described as such under the CDR Rules (in relation to a particular sector of the Australian economy).

Embedded Networks means a private electricity network where a parent connection point (which is connected to the NEM) distributes electricity through to one or more child connection points. Each child connect points is regarded as being 'off-market'. This type of network is managed by an 'embedded network operator'.

Financially Responsible Market Participant means an Electricity Retailer that take on, among other things, the market settlement responsibilities for the connection point of a customer.

Gateway means a person identified as a designated gateway in accordance with subsection 56AL(2) of the CCA.

Generally Available Plan means an energy plan available to small customers, except where specific restrictions apply.

Generic Product Data means all tariff data not relating to an identifiable person, including eligibility requirements for Hardship and Concessions linked to the product. This type of data has been identified as a Priority Energy Dataset.

Hardship refers to a policy that an Electricity Retailer has developed to identify and assist customers that experience financial payment difficult due to hardship as a result of a financial, health, family or other matter.

Market Settlement and Transfer Solutions means he procedures published by the AEMO under the NER, which include those governing the recording of financial responsibility for energy flows at a connection point, the transfer of that responsibility between market participants, and the recording of energy flows at a connection point.

Metering Data means data from all meter types for all connection points in the NEM which the AEMO receives: accumulated metering data, interval metering data, calculated metering data, substituted metering data, estimated metering data and check metering data. This type of data has been identified as a Priority Energy Dataset.

Metering Data Provider means a person who meets the requirements and is accredited and registered by the AEMO in that capacity, in accordance with the qualification process established under the NER.

Metering Installation Type means a meter installed to a connection to the network. There are seven different meter types, including smart meters. The meter types are set out in Chapter 7 of the NER.

National Electricity Market means the interconnection between five regional market jurisdictions, New South Wales (including the Australian Capital Territory), Queensland, South Australia, Tasmania and Victoria, for the distribution of electricity. Western Australia and Northern Territory are not connected to the NEM.

National Electricity Rules means version 138 of the rules which govern the operation of the NEM and is maintained by the AEMC.

National Energy Retail Law means the *National Energy Retail Law (South Australia) Act 2011* (SA) which came into effect on 1 July 2012 and implements the NECF together with the National Energy Retail Regulations and the National Energy Retail Rules.

National Energy Retail Regulations means the regulations known as *National Energy Retail Regulations* established under the NERL and section 12 of the *National Energy Retail Law (South Australia) Act 2011* (SA).

National Energy Retail Rules means the rules made by the AEMC (current version 20, 19 March 2020) and have the force of law under the NERL. These rules sit alongside the NER.

National Metering Identifier means a unique 10 or 11 digit number used to identify every electricity network connection point in NEM.

National Metering Identifier address means the physical location of the NMI connection point.

NMI Standing Data means the five MSATS master tables contain the standing data stored for each NMI (including information about the meter type, location and network tariffs). The five MSATS master tables are described in the AEMO's Standing Data for MSATS (version 5.0, 15 November 2019). NMI Standing Data has been identified as a Priority Energy Dataset.

Personal Information has the meaning given to that term in the Privacy Act.

Priority Energy Dataset means a type of dataset in relation to the NEM that has been identified by Treasury and agreed in-principle by the Treasurer of the Commonwealth Government on 9 January 2020. The scope and mix of these datasets are yet to be finalised and approved by the Commonwealth Government in the Designation Instrument for the energy CDR.

Privacy Act means the *Privacy Act 1988* (Cth).

Product Reference Data means data comprising information that identifies, describes or details products, including information such as tariffs, usage charges and applicable discounts where these products involve the supply of electricity to a customer (and includes Generic Product Data and Tailored Product Data). This type of data has been identified as a Priority Energy Dataset.

Register of Accredited Persons means the register of Accredited Persons maintained by the Accreditation Registrar in accordance with Subdivision B, Division 3 of Part IVD of the CCA.

Restricted Plan means an energy plan specifically targeted at an individual or exclusive group and tailored to the specific circumstances of that individual(s) and their need(s).

Tailored Product Data means all product data (including data from Restricted Plans) relating to an identifiable person, including eligibility requirement for Hardship and Concession linked to the product. This type of data has been identified as a Priority Energy Dataset.

Victorian Energy Retail Code means the code managed by the ESC which sets out the rules that electricity and gas retailers must follow when selling electricity and gas services to customers.

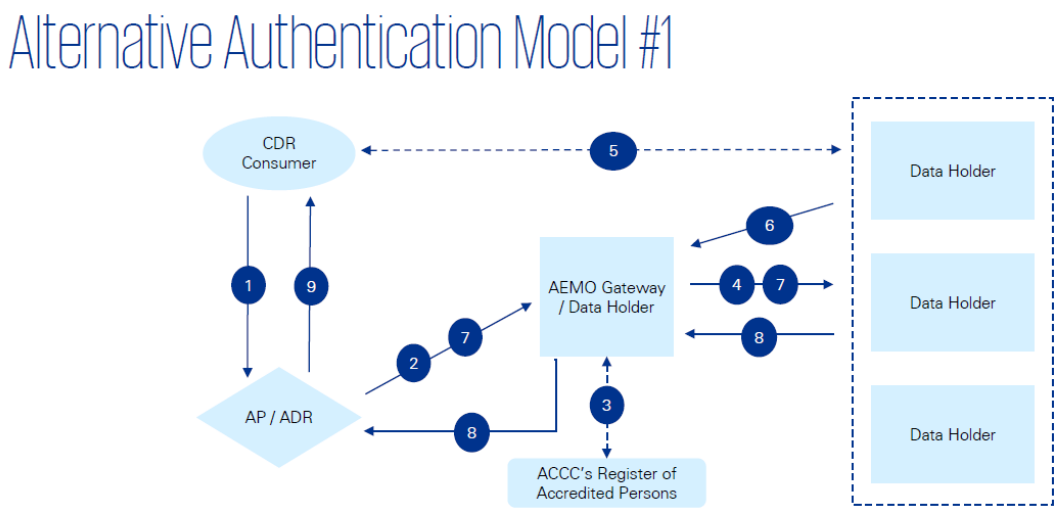
B. Abbreviations

ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ADR	Accredited Data Recipient
AEMC	Australian Energy Market Commission
AEMO	Australian Energy Market Operator Limited (ACN 072 010 327)
AER	Australian Energy Regulator
AP	Accredited Person
APP	Australian Privacy Principle
CCA	*Competition and Consumer Act 2010* (Cth)
CDR	Consumer Data Right regime
COAG	Council of Australian Governments
CSIRO	Commonwealth Scientific and Industrial Research Organisation
Data61	CSIRO's Data61
DELWP	Victorian Government's Department of Environment, Land, Water and Planning.
DER	Distributed Energy Resource
DH	Data Holder
DSB	Data Standards Body
EDR	External Dispute Resolution
EDSAC	Energy Data Standards Advisory Committee
EME	Energy Made Easy
energy sector	NEM
ESC	Victorian Essential Services Commission
FRMP	Financially Responsible Market Participant
MDP	Metering Data Provider
MSATS	Market Settlement and Transfer Solutions
NECF	National Energy Customer Framework
NEL	National Electricity Law
NEM	National Electricity Market
NER	National Electricity Rules
NMI	National Meter Identifier
OAIC	Office of the Australian Information Commissioner
OTP	One Time Password
PIA	Privacy Impact Assessment
PRD	Product Reference Data
PS	CDR Privacy Safeguard
Treasury	Commonwealth Department of the Treasury
VEC	Victorian Energy Compare
VERC	Victorian Energy Retail Code

Appendix 2: Diagrams of Data Flows

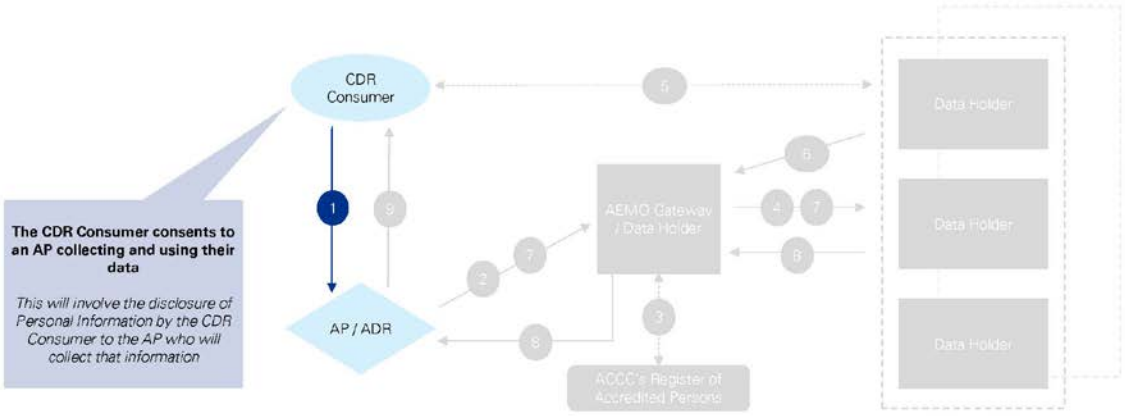
Note that both Alternative Authentication Model #1 and Alternative Authentication Model #2 have not yet been consulted on and may be amended by the ACCC. Other authentication models may also be considered.

A Alternative Authentication Model #1

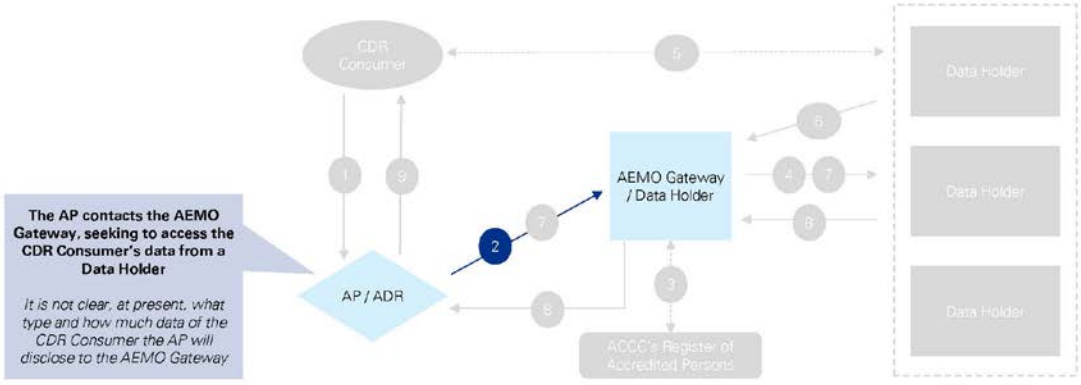


1. The CDR Consumer **consents** to an AP collecting and using their data to provide requested goods or services.
2. The AP contacts the AEMO Gateway, seeking to **access** the CDR Consumer's data from a Data Holder.
3. The AEMO Gateway **authenticates** the AP using the ACCC's Register of Accredited Persons.
4. The AEMO Gateway **identifies** the relevant Data Holder and **discloses** relevant Personal Information (if any) of the CDR Consumer for the Data Holder to **authenticate** the CDR Consumer.
5. The Data Holder sends a OTP to the CDR Consumer for **authentication** and also requests the CDR Consumer's **authorisation**. The CDR Consumer enters the OTP in the Data Holder's system.
6. The Data Holder confirms the **successful authentication** to the AEMO Gateway along with information linking the CDR Consumer to the relevant NMI.
7. The AP **requests** a specific set of CDR Data that is covered by the CDR Consumer's consent to the Data Holder via the AEMO Gateway.
8. The CDR Consumer's CDR Data is **disclosed** by the Data Holder to the AP via the AEMO Gateway.
9. The ADR provides the goods or services requested by the CDR Consumer.

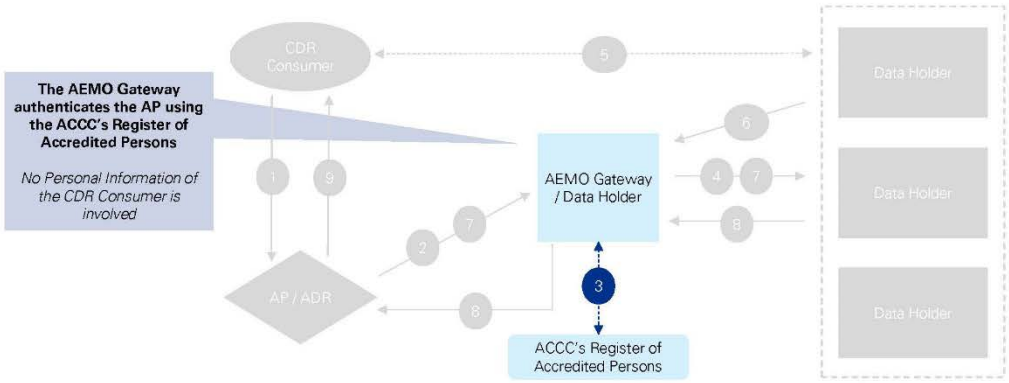
Alternative Authentication Model #1 - step 1



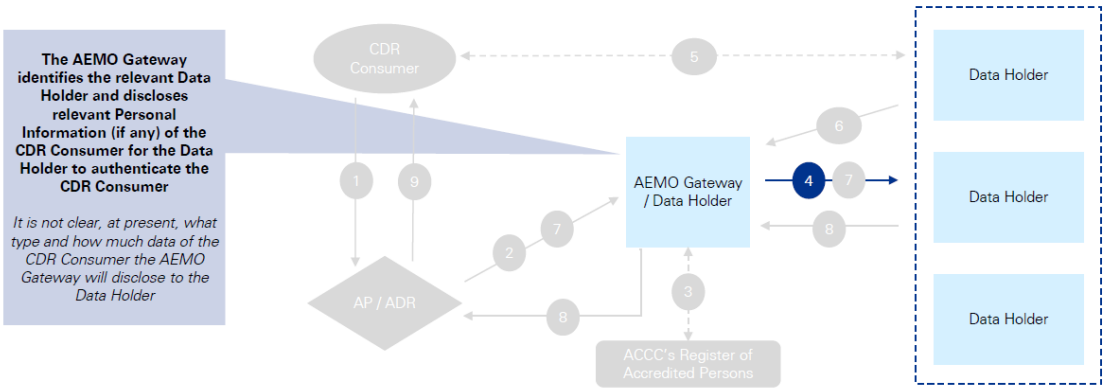
Alternative Authentication Model #1 - step 2



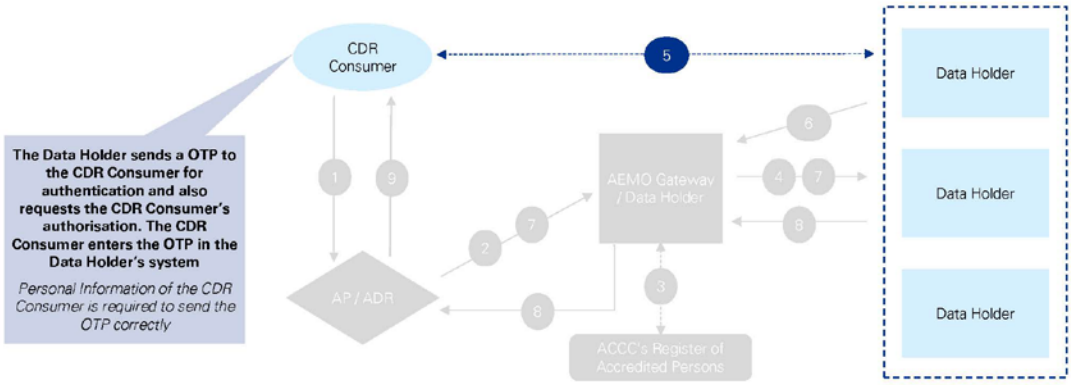
Alternative Authentication Model #1 - step 3



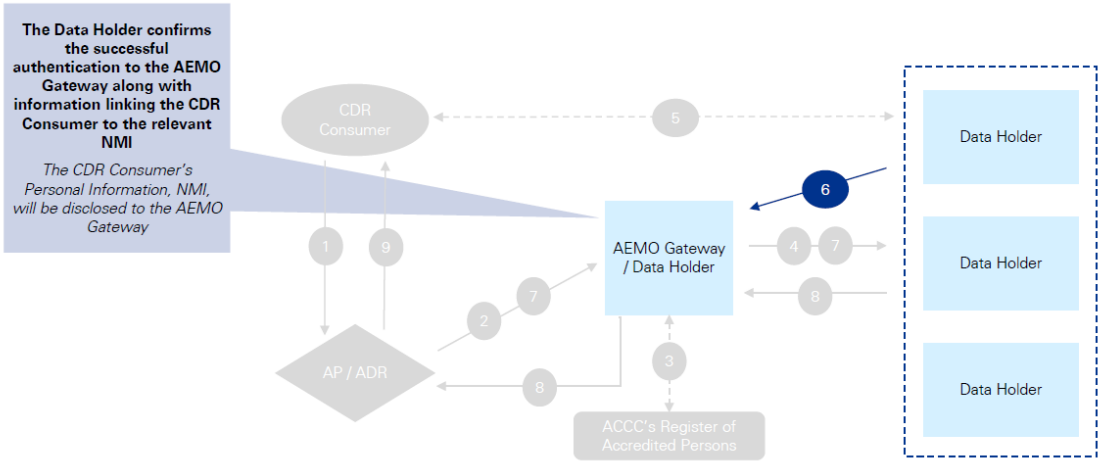
Alternative Authentication Model #1 - step 4



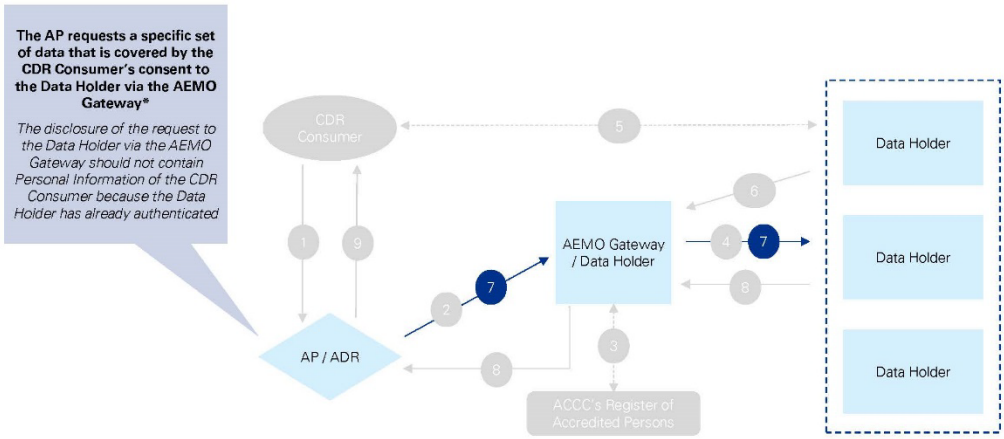
Alternative Authentication Model #1 - step 5



Alternative Authentication Model #1 - step 6

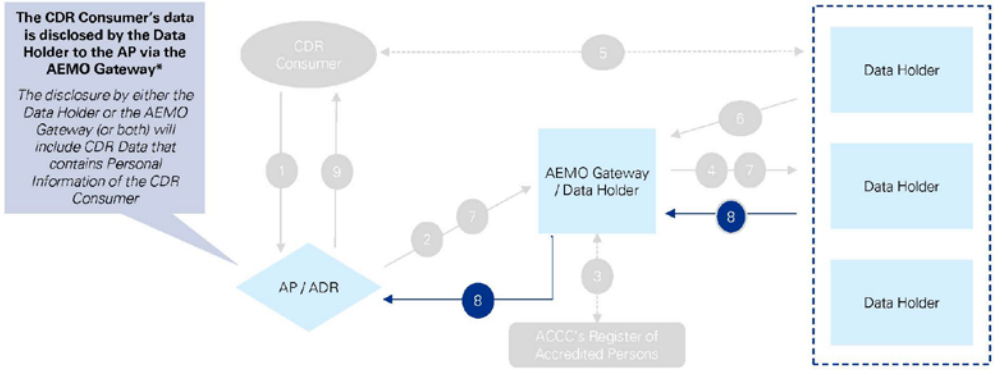


Alternative Authentication Model #1 - step 7



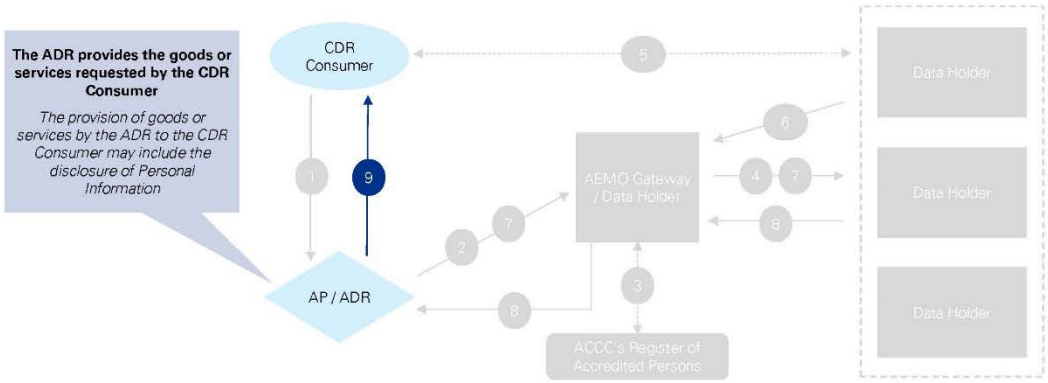
*Note that if the AEMO acts, depending on the Consumer Data Request, in the capacity of a Data Holder, the request may not need to be transmitted to the Data Holder

Alternative Authentication Model #1 - step 8

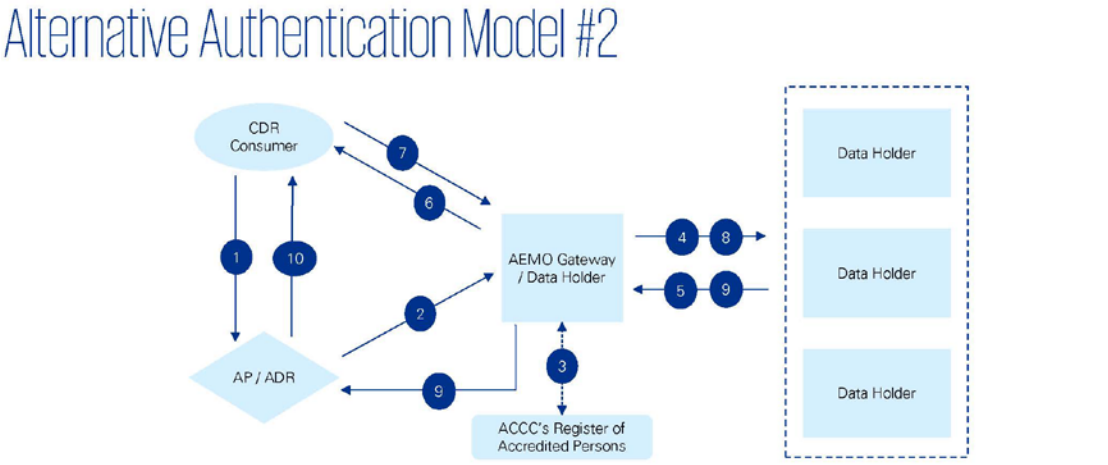


*Note that if the AEMO acts, depending on the Consumer Data Request, in the capacity of a Data Holder, CDR Data may only be disclosed by the AEMO Gateway and collected by the AP

Alternative Authentication Model #1 - step 9

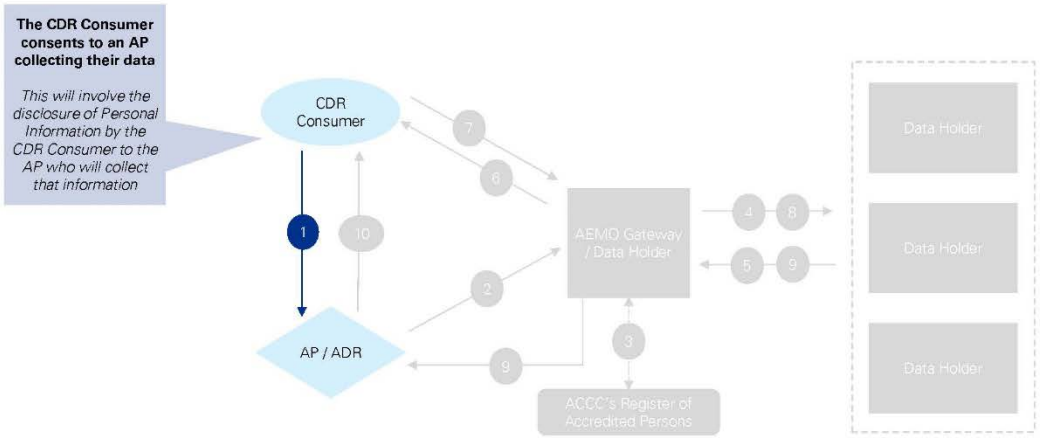


B Alternative Authentication Model #2

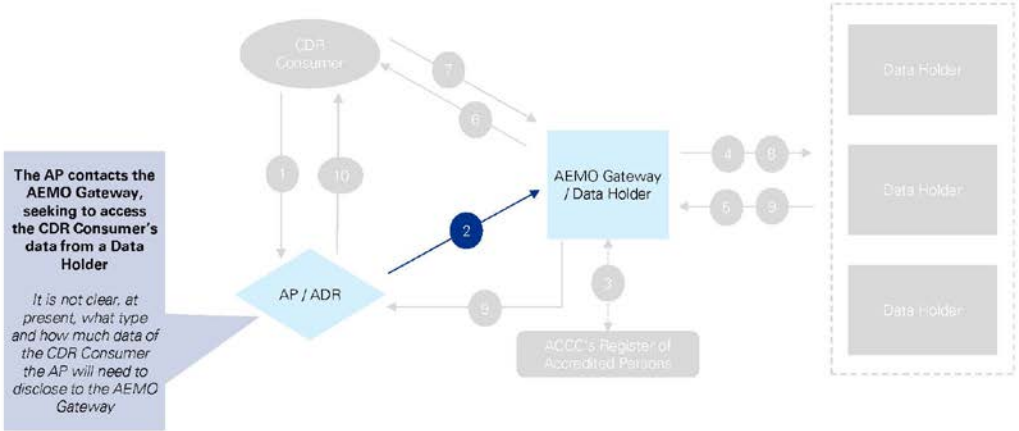


1. The CDR Consumer **consents** to an AP collecting and using their data for the purpose of providing goods or services.
2. The AP contacts the AEMO Gateway, seeking to **access** the CDR Consumer's data from a Data Holder.
3. The AEMO Gateway **authenticates** the AP using ACCC's Register of Accredited Persons.
4. The AEMO Gateway identifies the relevant Data Holder and **requests** CDR Consumer's contact information for authentication purposes.
5. The Data Holder **discloses** the CDR Consumer's contact information to the AEMO Gateway.
6. The AEMO Gateway **sends** the OTP to the CDR Consumer on behalf of the Data Holder, and **seeks** the CDR Consumer's authorisation too.
7. The CDR Consumer **enters** the OTP in the AEMO Gateway's system.
8. The AEMO Gateway **confirms** the authenticated request and provides the authorised request for CDR Data to the Data Holder. AEMO **may retain** the authentication to avoid persistent verifications for CDR Consumers.
9. The CDR Consumer's data is **disclosed** to the AP via the AEMO Gateway.
10. The ADR provides the goods or services requested by the CDR Consumer.

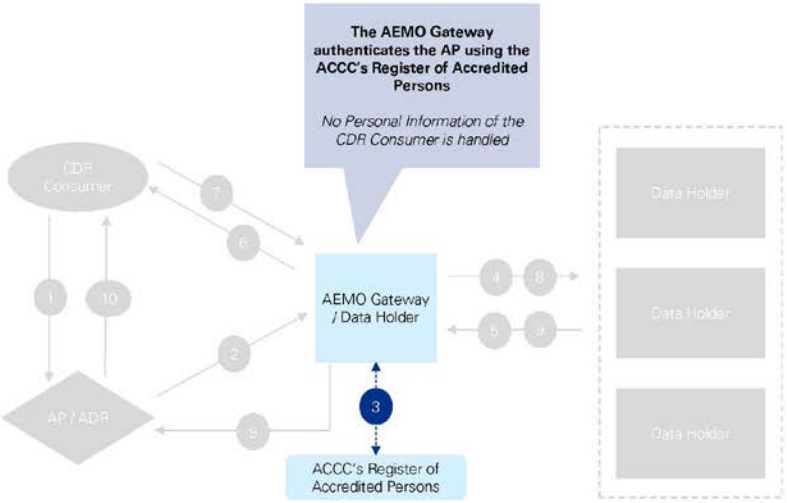
Alternative Authentication Model #2 - step 1



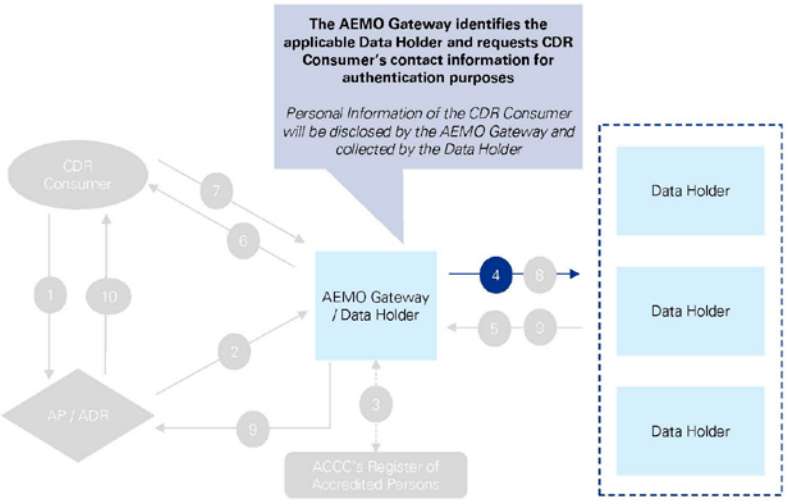
Alternative Authentication Model #2 - step 2



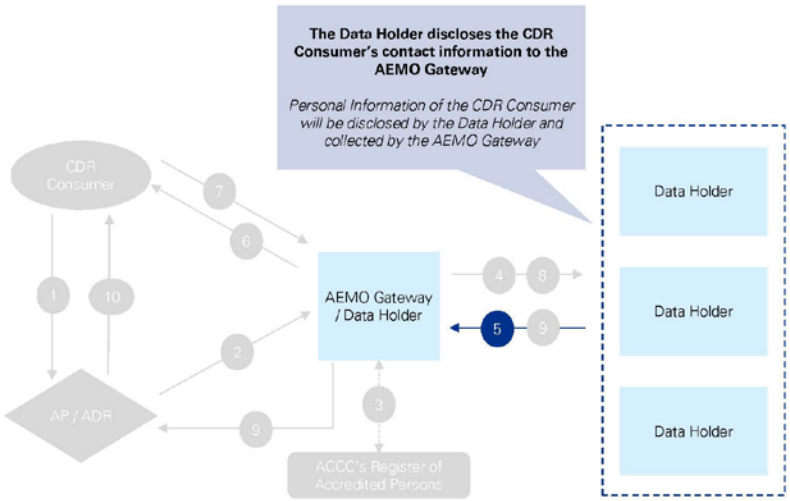
Alternative Authentication Model #2 - step 3



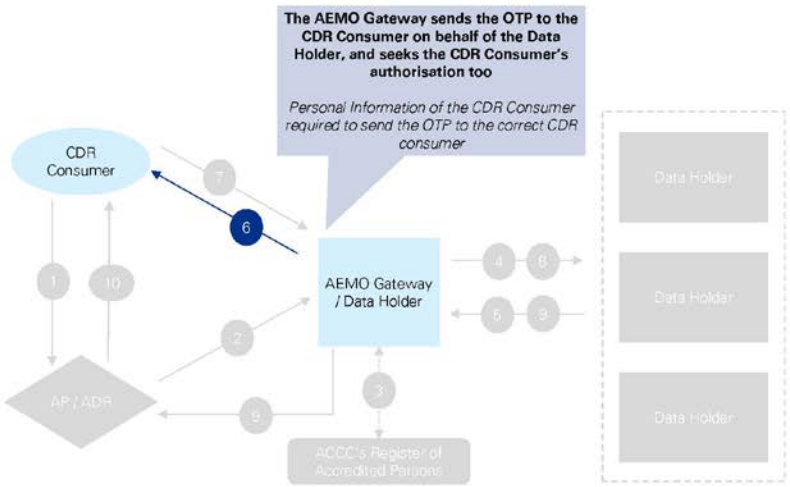
Alternative Authentication Model #2 - step 4



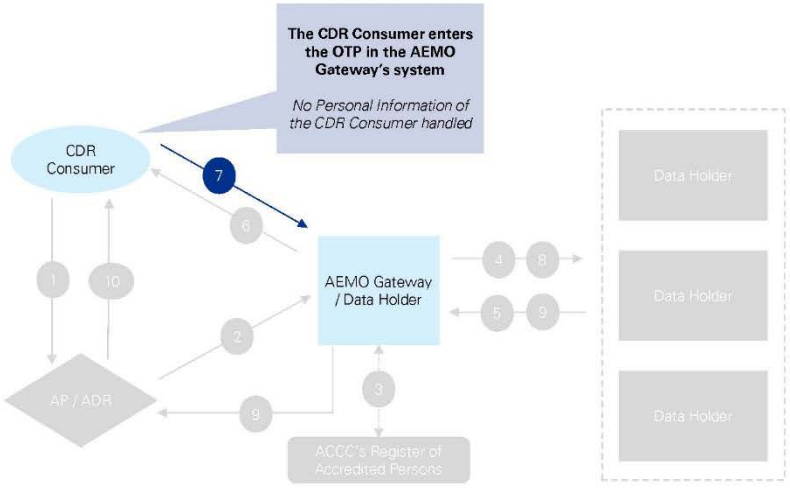
Alternative Authentication Model #2 - step 5



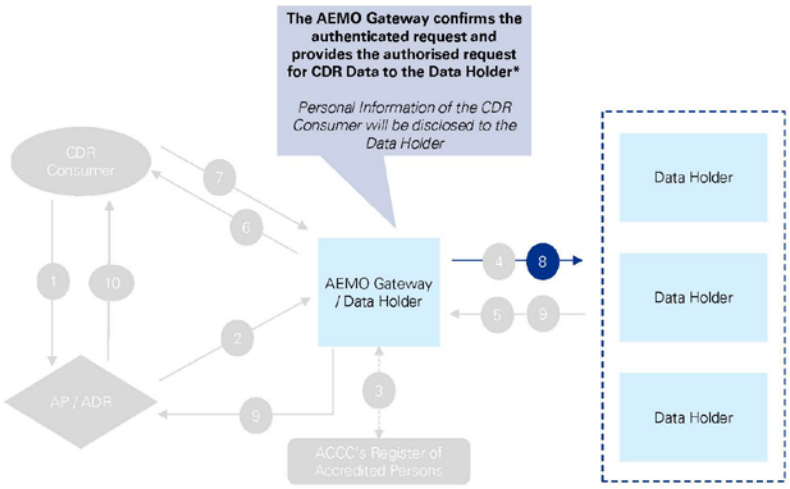
Alternative Authentication Model #2 - step 6



Alternative Authentication Model #2 - step 7

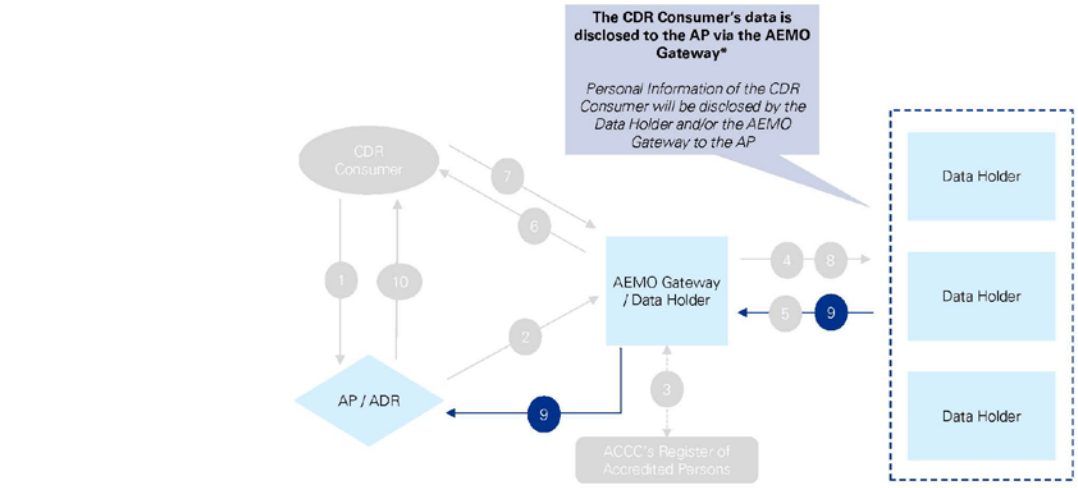


Alternative Authentication Model #2 - step 8



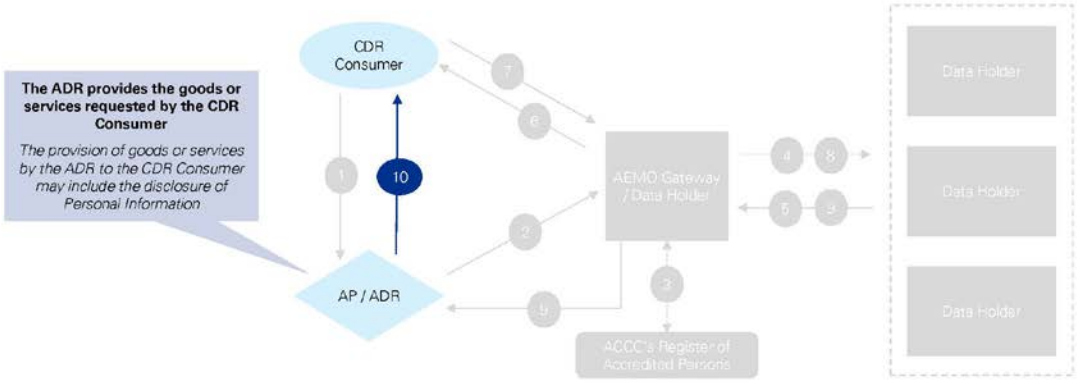
*Note that if the AEMO acts, depending on the Consumer Data Request, in the capacity of a Data Holder, the request may not need to be transmitted to the Data Holder

Alternative Authentication Model #2 - step 9



*Note that if the AEMO acts, depending on the Consumer Data Request, in the capacity of a Data Holder, CDR Data may only be disclosed by the AEMO Gateway and collected by the AP

Alternative Authentication Model #2 - step 10



Appendix 3: List of Materials Reviewed

We reviewed the following key materials while preparing this SPIA.

a) *Competition and Consumer Act 2010* (Cth).

b) *Privacy Act 1988* (Cth).

c) Lockstep Consulting's Review of the Consumer Data Right PIA – Consulting Report, version 1.0, January 2019.

d) Treasury's Privacy Impact Assessment, Consumer Data Right, 1 March 2019 (including relevant submissions from energy sector participants that were received by Treasury to produce the PIA).

e) Maddocks' PIA Report on the Consumer Data Right Regime for Treasury, 29 November 2019.

f) Treasury's (including the ACCC, the OAIC and CSIRO's Data61) Consumer Data Right Privacy Impact Assessment Agency Response, December 2019.

g) Competition and Consumer (Consumer Data Right) Rules 2020, 4 February 2020.

h) OAIC's CDR Privacy Safeguard Guidelines, February 2020.

i) CSIRO Data61's Consumer Data Standards, version 1.3.0, 17 April 2020.

j) CSIRO Data61's Consumer Experience (CX) Standards, version 1.3.0, 17 April 2020.

k) CSIRO Data61's Consumer Experience (CX) Guidelines, version 1.3.0, 17 April 2020.

l) CSIRO Data61's Consumer Experience Research Phase 3: Round 1 and 2, March 2020.

m) ACCC's Consumer Data Right in Energy Position Paper: Data Access Model for Energy Data, August 2019 (including relevant submissions from energy sector participants to the 25 February 2019 consultation by the ACCC on Data Access Models for Energy Data).

n) Treasury's Priority Energy Datasets Consultation, Consumer Data Right, 29 August 2019 (including relevant submissions from energy sector participants received by Treasury in response to this Consultation).

o) Minutes from the CSIRO Data61's EDSAC meetings, up until 11 March 2020.

p) PIA undertaken by Lockstep Consulting for DELWP on Advanced Metering Infrastructure, August 2011.

Appendix 4: List of Stakeholders Consulted

We consulted the following stakeholders while preparing this SPIA. We acknowledge each stakeholder's contribution and appreciate their support.

a) AGL Energy Ltd.

b) Australian Competition and Consumer Commission.

c) Australian Department of Industry, Science, Energy and Resources.

d) Australian Department of Treasury.

e) Australian Energy Market Operator.

f) Australian Energy Regulator, including Energy Made Easy.

g) Commonwealth Scientific and Industrial Research Organisation's Data61.

h) Consumer Policy Research Centre.

i) Energy Consumers Australia.

j) Energy OS Pty Ltd.

k) Energy Queensland, including Ergon Energy.

l) Energy Water Ombudsmen – New South Wales, Queensland, South Australia and Victoria.

m) Hive Empire Pty Ltd, trading as finder.com.au.

n) Office of the Australian Information Commissioner.

o) Victorian Department of Environment, Land, Water and Planning, including Victorian Energy Compare.