



Maddocks



Department of the Treasury

CONSUMER DATA RIGHT REGIME

Update 4 to Privacy Impact Assessment

Date of analysis: 26 October 2021

Report finalised on 29 October 2021

This document has been prepared for the Department of the Treasury. No other reader should rely on the material in this document without seeking legal advice.

Contents

Part A	INTRODUCTION	3
1.	Overview	3
2.	Structure of, and approach to, this PIA Update 4 Report	4
Part B	EXECUTIVE SUMMARY	6
3.	Introduction	6
4.	Summary of findings	6
5.	Recommendations	7
Part C	METHODOLOGY	9
6.	Our methodology	9
7.	Scope of this PIA Update 4 Report	10
Part D	PROJECT DESCRIPTION	11
8.	Overview	11
Part E	ANALYSIS OF RISKS	15
9.	Introduction	15
10.	General impacts	15
11.	Risks associated with the role and obligations of AEMO	16
12.	Risks associated with the role and obligations of Retail Data Holders	24
13.	Risks associated with the scope of energy sector data	26
14.	Impact of CDR Consumers in the energy sector being unable to make Direct to Consumer Requests	28
15.	Individuals, who are not the CDR Consumer making the Consumer Data Request, being the subject of CDR Data	29
Part F	GLOSSARY	31
Part G	LIST OF SUBMISSIONS	33

Part A INTRODUCTION

1. Overview

- 1.1 On 11 December 2019, the Department of the Treasury (**Treasury**) published the Privacy Impact Assessment into the Consumer Data Right Regime (**Original CDR PIA report**), together with the responses to the recommendations made in that report.¹
- 1.2 As the Original CDR PIA report was undertaken as a “point in time” analysis of the development of the legislative framework (that is, the *Competition and Consumer Act 2010 (Cth)* (**CC Act**), *Competition and Consumer (Consumer Data Right) Rules 2020 (Cth)* (**CDR Rules**), Data Standards and the Open Banking Designation), the Original CDR PIA report recommended that it be treated as a “living document”, which should be further updated and/or supplemented as the various components of the legislative framework are amended and/or developed.²
- 1.3 Responsibility for making the CDR Rules, including continually reviewing, considering and revising those CDR Rules as required, has now passed from the Australian Competition and Consumer Commission (**ACCC**) to the Minister for Superannuation, Financial Services and the Digital Economy (**Minister**).
- 1.4 The CDR Rules commenced on 6 February 2020. Since that time, the ACCC and Treasury have undertaken several privacy impact update processes to analyse the impact of any proposed amendments to the CDR Rules (**PIA Update reports**).
- 1.5 In accordance with the recommendation in the Original CDR PIA report, Maddocks has been engaged by Treasury to consider the privacy impacts of a further round of proposed amendments to the CDR Rules, insofar as they relate to the energy sector, and prepare this fourth updated privacy impact assessment report (**PIA Update 4 Report**).
- 1.6 The PIA Update 4 process has been a systematic assessment of the proposed amendments to the CDR Rules for the energy sector, identifying the potential impact that these amendments might have on the privacy of individuals, and setting out recommendations for managing, minimising or eliminating that impact.³
- 1.7 This PIA Update 4 Report is designed to:
 - 1.7.1 assist Treasury in identifying and assessing any potential privacy risks to individuals presented by particular proposed amendments to the CDR Rules, so that those risks can be properly considered, and then balanced against all other relevant considerations and benefits associated with the proposed amendments;
 - 1.7.2 present options that could be implemented to reduce or eliminate any identified potential privacy risks, in the form of recommendations for consideration by Treasury; and
 - 1.7.3 illustrate the focus and value being given to privacy risks and risk mitigation.

¹ The Original CDR PIA report, and the responses made to the recommendations in that report, are available at: <https://treasury.gov.au/publication/p2019-41016>.

² Recommendation 1 in the Original CDR PIA report.

³ *Guide to undertaking privacy impact assessments (May 2020)*, published by the Office of the Australian Information Commissioner (**OAIC**) (<https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>).



- 1.8 We have based our discussion and analysis in this PIA Update 4 Report on a consolidated version of the draft CDR Rules (version 40) provided to us by Treasury on 25 October 2021.
- 1.9 Version 40 of the draft CDR Rules reflects:
- 1.9.1 the roles and obligations of the Australian Energy Market Operator Limited (**AEMO**) as a Data Holder;
 - 1.9.2 the roles and obligations of Retail Data Holders; and
 - 1.9.3 the introduction of the concept of Primary and Secondary Data Holders, which in the energy sector will mean that a Primary Data Holder (i.e. a retail energy provider) will request CDR Data from a Secondary Data Holder (AEMO) to fulfil a Consumer Data Request (this has also been referred to as Peer-to-Peer (**P2P**) model⁴).
- 1.10 We note that Version 40 of the CDR Rules also includes a number of proposed amendments that are not specific to the energy sector. These proposed amendments have not been considered as part of this PIA Update 4 Report.

2. Structure of, and approach to, this PIA Update 4 Report

- 2.1 This PIA Update 4 Report should be read in conjunction with the relevant amendments in version 40 of the CDR Rules⁵.
- 2.2 This PIA Update 4 Report is comprised of the following sections:
- 2.2.1 **Part A – Introduction:** This section describes the PIA processes that have been undertaken to date, explains the purpose of this PIA Update 4 Report, and introduces the key changes that will be introduced if the proposed amendments to the CDR Rules are made.
 - 2.2.2 **Part B – Executive Summary:** This section contains a summary of the privacy risks we have identified, together with a list of all recommendations we have made as a result of our analysis.
 - 2.2.3 **Part C – Methodology:** This section details how we have undertaken this PIA Update 4 Report, and includes information about the scope of this PIA Update 4 Report.
 - 2.2.4 **Part D – Project Description:** This section contains a high-level summary of the further proposed changes to the CDR Rules and discusses the various concepts and information flows relevant to those proposed changes.
 - 2.2.5 **Part E – Analysis of Risks:** This section sets out our analysis of the potential privacy risks that we have identified as being associated with the proposed changes to the CDR Rules. We have identified current mitigation strategies and conducted a gap analysis to identify any areas of concern, and included recommendations to mitigate any privacy risks.
 - 2.2.6 **Part F – Glossary:** This section sets out a list of capitalised terms that we have used in this PIA Update 4 Report, and their definitions.

⁴ The Peer-to-Peer data access model is explained in the *Peer-to-peer data access model in the energy sector – CDR Rules and standards design paper*, 30 April 2021.

⁵ The relevant amendments were shown in green text by the drafters, for ease of reference.



- 2.2.7 **Part G – List of Submissions:** This section contains a list of stakeholders who provided written submissions as part of Treasury’s stakeholder consultation process, which we have considered as part of this PIA Update 4 process.



Part B EXECUTIVE SUMMARY

3. Introduction

- 3.1 In this **Part B [Executive Summary]**, we have provided a summary of the privacy risks we have identified in the proposed changes to the CDR Rules, as well as a consolidated list of all of the recommendations we have made as a result of our analysis to address privacy risks that we have identified.
- 3.2 We understand that Treasury, in consultation with the Minister and other Commonwealth agency stakeholders as required, will separately develop a response to our recommendations.

4. Summary of findings

- 4.1 The application of the CDR Rules (including the proposed amendments) is likely to have some privacy impacts that are specific to the energy sector. The proposed amendments do include a number of important additional protections for CDR Consumers in relation to CDR Data in the energy sector. In addition, over the course of the development of the proposed amendments to the CDR Rules, we have been very pleased to note how some strategies, particularly designed to mitigate identified privacy impacts, have been included or strengthened in the CDR Rules as the drafting of the amendments has progressed over time.
- 4.2 However, we consider that there may be some residual privacy impacts which could potentially be further mitigated to enhance the protections for CDR Consumers. These potential privacy impacts are discussed in detail in **Part E [Analysis of Risks]**, but include the following:

General

- 4.2.1 As we have raised in other PIA Update reports, we consider that the complexity of the framework underpinning the CDR regime means that entities participating in the CDR regime (such as Retail Data Holders and AEMO) and CDR Consumers may not understand, or take steps to action, their obligations or rights under the legislative framework.

The role of AEMO

- 4.2.2 If AEMO receives personal information from a Retail Data Holder in connection with a Consumer Data Request (or AEMO's data holdings change), and this results in AEMO holding CDR Data from which a CDR Consumer could be identified, AEMO will not be subject to all of the ordinary obligations of Data Holders.
- 4.2.3 Given the unique role of AEMO in the energy sector, CDR Consumers may not understand the involvement of AEMO when giving their consents and authorisations.
- 4.2.4 AEMO will be authorised, but not required, to provide data to Retail Data Holders on request (i.e. because a Retail Data Holder is seeking to fulfil a Consumer Data Request). This means that CDR Consumers may not be able to access all relevant CDR Data.

- 4.2.5 If AEMO discloses data to a retailer that is not a Retail Data Holder for the purposes of the CDR regime, this will disclose CDR Data outside the CDR regime.

Direct to Consumer Requests

- 4.2.6 Under the proposed amendments to the CDR Rules, CDR Consumers will not be able to directly access their energy sector data from a Retail Data Holder or AEMO (although they will continue to be able to access much of this data under the National Energy Customer Framework or the Victorian energy retail regulation).

5. Recommendations

Recommendation 1

As raised in previous PIA Update reports, it will be very important that all entities participating in the CDR regime (such as Retail Data Holders and AEMO) understand, and take steps to action, their obligations under the legislative framework. In addition, it will be important that CDR Consumers understand their rights under the CDR regime.

Accordingly, we recommend that Treasury arrange for detailed, comprehensive and clear guidance about the intended application of the CDR Rules, as amended by the proposed changes, to be issued. We suggest that specific guidance could be developed to assist CDR Consumers, AEMO and Retail Data Holders.

Recommendation 2

We recommend that, before commencement of the amendments to the CDR Rules, Treasury confirm that the Data Standards do (or will) prohibit Retail Data Holders from disclosing information to AEMO about CDR Consumers if that information would allow AEMO to identify one or more CDR Consumers for the data held by AEMO.

Recommendation 3

We recommend that Treasury consider whether it would be appropriate to make CDR Consumers aware of the involvement of AEMO in respect of the fulfilment of Consumer Data Requests, or whether this would risk 'information overload' for CDR Consumers or be otherwise unnecessary. This may involve the Data Standards Body undertaking consumer research as required.

Recommendation 4

The proposed amendments to the CDR Rules will authorise AEMO to disclose CDR Data to a Retail Data Holder, but will not require AEMO to do so. While the risks of a CDR Consumer not being able to access all of their CDR Data may be low for the energy sector in circumstances where there is only one Secondary Data Holder (AEMO), we recommend that Treasury consider whether further amendments to the CC Act should be proposed in future to mitigate this risk, if the P2P model is to be applied to other designated sectors.

Recommendation 5

We recommend that Treasury satisfy itself that AEMO's existing mechanisms will enable it to determine whether a retailer is a Retail Data Holder for the purposes of the CDR regime. In particular, we are considering recommending that Treasury satisfy itself that AEMO will have access to real-time information about whether, at any given point in time, a retailer is a Retail Data Holder for the purposes of the CDR regime.

Recommendation 6

We recommend that:

- Treasury consider whether it is appropriate to build flexibility into the CDR Rules so that all of the obligations on Data Holders, including the obligation to comply with all of the Privacy Safeguards, will automatically apply to AEMO if it holds CDR Data from which it could identify a CDR Consumer; and/or
- AEMO be required to:
 - implement processes and systems to be able to identify if it does become the holder of CDR Data from which a CDR Consumer could be identified by AEMO; and
 - notify the CDR regulators if this occurs, so that appropriate steps can be taken as a result, if required.

Recommendation 7

We recommend that, as part of further consideration of Direct to Consumer requests in the energy sector, a detailed analysis be undertaken to determine the differences (if any) in the data that CDR Consumers can currently access under existing mechanisms, and the CDR Data that CDR Consumers would be able to access if they could make Direct to Consumer Requests. This analysis would assist all parties to understand the potential benefits for CDR Consumers in being able to make Direct to Consumer requests.



Part C METHODOLOGY

6. Our methodology

6.1 We conducted our PIA Update 4 process broadly in accordance with the OAIC’s *Guide to undertaking privacy impact assessments*. This involved the following steps:

Stage	Description of steps
1.	<p>Plan for the PIA Update 4 Report: We were provided with initial instructions about the proposed amendments to the CDR Rules, including in an initial workshop with Treasury. We were provided with the drafting instructions to amend the CDR Rules, to assist us to gain an understanding of Treasury’s intentions for the proposed amendments to the CDR Rules.</p> <p>We also agreed on the scope of this PIA Update 4 Report (discussed further in this Part C [Methodology] below), the approach to undertaking stakeholder consultation, and the timeframes for the necessary activities involved in conducting this PIA Update 4 Report.</p>
2.	<p>Privacy impact analysis and compliance check: In this stage, we identified and critically analysed how the proposed amendments to the CDR Rules will impact upon privacy, both positively and negatively.</p> <p>For the reasons elaborated in the Original PIA report, we took the same approach to risk assessment which was adopted in the original CDR regime analysis, and have not endeavoured to quantify or label the level of risk associated with each of the identified privacy impacts.</p>
3.	<p>Privacy management and addressing risks: We considered potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.</p>
4.	<p>Recommendations: From the stages referred to above, we prepared indications of potential recommendations to remove or reduce identified avoidable privacy risks.</p>
5.	<p>Draft issues paper: From the stages referred to above, we prepared a draft issues paper to assist Treasury with its stakeholder consultation process.</p>
6.	<p>Stakeholder consultation: Treasury published a draft of the proposed legislative instrument to amend the CDR Rules, with an invitation to members of the public to provide written submissions to either or both documents. Treasury provided us with those submissions, from which we identified further valuable insights.</p>
7.	<p>Privacy management and addressing risks: We further refined the potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.</p>
8.	<p>Recommendations: From the stages referred to above, we prepared recommendations to remove or reduce identified avoidable privacy impacts.</p>
9.	<p>Report: We finalised this PIA Update 4 Report.</p>
10.	<p>Respond and review: We understand that Treasury will review this PIA Update 4 Report, in consultation with other stakeholders as required, to include responses to our recommendations.</p>



7. Scope of this PIA Update 4 Report

- 7.1 The scope of this PIA Update 4 Report is limited to the proposed changes to the CDR Rules and the proposed amendments to the *Competition and Consumer Regulations 2010* (Cth) (**CDR Regulations**), insofar as they relate to the energy sector, as described in **Part D [Project Description]**. As discussed above, we only considered the energy-specific amendments in version 40 of the draft CDR Rules, and the exposure draft of version 4 of the CDR Regulations (with a further minor amendment notified to us by Treasury on 21 October 2021).
- 7.2 As was the case with the Original PIA report, this PIA Update 4 Report does not include consideration of any possible future versions of the CDR Rules or the Data Standards.

Part D PROJECT DESCRIPTION

8. Overview

- 8.1 The proposed amendments to the CDR Rules will, if passed, introduce (among other things) the concept of:
- 8.1.1 shared responsibility data (**SR Data**), which, in relation to a CDR Consumer and a designated sector, will have the meaning set out in the relevant sector-specific schedule to the CDR Rules (see proposed definition in Rule 1.7);
 - 8.1.2 **SR Data Requests**, which will be Consumer Data Requests for CDR Data that is, or will include, the SR Data of a CDR Consumer (see proposed definition in Rule 1.7);
 - 8.1.3 **Primary Data Holders**, which, in relation to SR Data and a designated sector, will mean the Data Holder specified in the relevant sector-specific schedule to the CDR Rules as being the Primary Data Holder for the SR Data (see proposed definition in Rule 1.7); and
 - 8.1.4 **Secondary Data Holders**, which, in relation to SR Data and a designated sector, will mean the Data Holder specified in the relevant sector-specific schedule to the CDR Rules as being the Secondary Data Holder for the SR Data (see proposed definition in Rule 1.7).
- 8.2 Importantly, proposed Schedule 4 to the CDR Rules sets out a number of provisions that are specific to the energy sector. These provisions, amongst other things:
- 8.2.1 define SR Data for the purposes of the energy sector;
 - 8.2.2 define Primary Data Holders for the purposes of the energy sector;
 - 8.2.3 clarify that the only Secondary Data Holder in the energy sector is AEMO; and
 - 8.2.4 set out the roles and responsibilities of Retail Data Holders and AEMO.

Definition of SR Data

- 8.3 Proposed Rule 4.3 of Schedule 4 defines SR Data in the energy sector as meaning AEMO Data in relation to a CDR Consumer. Proposed Rule 1.2 of Schedule 4 defines AEMO Data as:
- 8.3.1 in relation to an electricity retailer, the following information that relates to an arrangement with the retailer:
 - (a) national metering identifier (**NMI**) standing data;
 - (b) metering data; or
 - (c) distribution energy resources (**DER**) register data; and
 - 8.3.2 in relation to a CDR Consumer, the above data that relates to an arrangement relevant to the CDR Consumer.



Definition of Retail Data Holders

- 8.4 Proposed Rule 4.3 of Schedule 4 provides that a Primary Data Holder for SR Data is the CDR Consumer's retail energy provider. For ease of reference, in this PIA Update 4 Report we have referred to Primary Data Holders in the energy sector as **Retail Data Holders**⁶.

CDR Consumers making requests for SR Data

- 8.5 Proposed Rule 1.22(2) means that SR Data Requests can only be made by a CDR Consumer to a Primary Data Holder, using the Primary Data Holder's direct request service. However, CDR Consumers in the energy sector will not be able to make Direct to Consumer Requests as proposed Rule 8.5 of Schedule 4 provides that Part 3 of the CDR Rules does not apply in relation to energy sector data.
- 8.6 Proposed Rule 1.19 means that if a CDR Consumer can make an SR Data Request to a Primary Data Holder, the CDR Consumer is not eligible to make or initiate a SR Data Request for that SR Data to the Secondary Data Holder.
- 8.7 In the energy sector, this means that CDR Consumers will only be able to make SR Data Requests to Retail Data Holders, and not to AEMO.
- 8.8 Proposed Rule 1.20(1) effectively requires Retail Data Holders to provide a Consumer Data Request Service for any SR Data. Additionally, proposed Rule 1.21 requires Retail Data Holders to provide a Consumer Dashboard (in accordance with Rule 1.15) in relation to an SR Data Request as if the Retail Data Holder held the requested SR Data.
- 8.9 Additionally, proposed Rule 1.20(2) requires Secondary Data Holders to, in respect of SR Data, provide an online service that:
- 8.9.1 can be used by the Primary Data Holder to request any SR Data needed to respond to an SR Data Request from the Secondary Data Holder;
 - 8.9.2 enables the requested SR Data to be disclosed to the Primary Data Holder in machine-readable form; and
 - 8.9.3 conforms with the Data Standards.

Responding to SR Data Requests by CDR Consumers

- 8.10 In accordance with proposed Rule 1.22(3), a Retail Data Holder must, using the online service provided by AEMO, and otherwise in accordance with the Data Standards, request AEMO to disclose any SR Data that the Retail Data Holder needs to respond to a SR Data Request made by a CDR Consumer.
- 8.11 Relevantly, if AEMO chooses:
- 8.11.1 to disclose the requested SR Data to the Retail Data Holder, it must do so in accordance with any relevant Data Standards (proposed Rule 1.22(4)); or
 - 8.11.2 not to disclose the requested SR Data to the Retail Data Holder, it must notify the Retail Data Holder of its refusal (proposed Rule 1.22(5)).
- 8.12 Finally, pursuant to proposed Rule 1.22(6), the Retail Data Holder must comply with Rule 3.4 (disclosing CDR Data in response to a Consumer Data Request) and Rule 3.5 (refusing to disclose CDR Data) as if it were the Data Holder for any SR Data covered by the SR Data Request. However, proposed Rule 1.22(7) means that the Retail Data Holder does not have

⁶ We note that the proposed amendments in the CDR Rules refer to Retail Data Holders as 'retailers'.



to comply with Rule 3.4(3) in relation to any SR Data that AEMO has refused to disclose to the Retail Data Holder.

Accredited Persons making requests for SR Data

- 8.13 Proposed Rule 1.23(2) means that SR Data Requests can be made by an Accredited Person to a Retail Data Holder using the Retail Data Holder's Accredited Person request service.

Responding to SR Data Requests by Accredited Persons

- 8.14 Proposed Rule 1.23(3) means that Retail Data Holders must comply with Rule 4.5 (asking CDR Consumer for authorisation to disclose CDR Data) as if the Retail Data Holder were the Data Holder for any SR Data covered by the SR Data Request.

- 8.15 If the CDR Consumer authorises the disclosure of the relevant SR Data, proposed Rule 1.23(4) will require the Retail Data Holder to, using the online service provided by AEMO and otherwise in accordance with the Data Standards, request AEMO to disclose any SR Data that the Retail Data Holder needs to respond to a SR Data Request made by a CDR Consumer.

- 8.16 Relevantly, if AEMO chooses:

8.16.1 to disclose the requested SR Data to the Retail Data Holder, it must do so in accordance with any relevant Data Standards (proposed Rule 1.23(5)); or

8.16.2 not to disclose the requested SR Data to the Retail Data Holder, it must notify the Retail Data Holder of its refusal (proposed Rule 1.23(6)).

- 8.17 Finally, pursuant to proposed Rules 1.23(7) and (9), the Retail Data Holder must comply with Rule 4.6 (disclosing CDR Data in response to a Consumer Data Request) and Rule 4.7 (refusing to disclose CDR Data) as if it were the Data Holder for any SR Data covered by the SR Data Request. However, proposed Rule 1.23(8) will mean that the Retail Data Holder does not have to comply with Rule 4.6(4) in relation to any SR Data that AEMO refused to disclose to the Retail Data Holder.

- 8.18 Additionally, pursuant to:

8.18.1 proposed Rule 1.23(10), Rule 4.13 (withdrawal of consent) will apply as if the Retail Data Holder were the Data Holder for any SR Data covered by the SR Data Request;

8.18.2 proposed Rule 1.23(11), Division 4.4 (authorisations to disclose CDR Data) will apply as if:

(a) a reference to the Data Holder were a reference to the Retail Data Holder; and

(b) proposed Rule 4.25(3) were included, noting that the proposed rule provides that for Rule 4.25(2)(a), giving effect to a withdrawal includes cancelling any current requests to AEMO by the Retail Data Holder under proposed Rule 1.23(4).

Restrictions on the use of SR Data

- 8.19 Proposed Rule 1.24(1) will mean that a Retail Data Holder must not use AEMO's service other than to request the SR Data that it needs to respond to an SR Data Request.

- 8.20 Additionally, proposed Rule 1.24(1) will mean that if AEMO provides SR Data to a Retail Data Holder in response to a request:



- 8.20.1 the Retail Data Holder must not use or disclose the SR Data for a purpose other than responding to the relevant SR Data Request; and
- 8.20.2 once the Retail Data Holder has responded to the relevant SR Data Request, it must delete any of the SR Data that it holds in accordance with the CDR Data deletion process.

Managing unsolicited SR Data

- 8.21 Proposed Rule 1.25 will mean that a Retail Data Holder must destroy SR Data as soon as practicable if it:
 - 8.21.1 collects SR Data from AEMO, purportedly under the CDR Rules, but not actually as the result of seeking to collect the SR Data under the CDR Rules; and
 - 8.21.2 is not required to retain that SR Data by, or under, an Australian law or a court/tribunal order.

Record-keeping obligations

- 8.22 It is proposed that Rule 9.3(1) will be amended to require:
 - 8.22.1 Retail Data Holders to keep and maintain records that explain:
 - (a) any requests for SR Data made by the Retail Data Holder under proposed Rule 1.23(4); and
 - (b) responses to those requests received under proposed Rules 1.23(5) or (6); and
 - 8.22.2 AEMO to keep and maintain records that explain:
 - (a) any requests for SR Data received under proposed Rule 1.22(3) or proposed Rule 1.23(4);
 - (b) any responses to requests, given under proposed Rules 1.22(4) or (5) or proposed Rules 1.23(5) or (6); and
 - (c) if they have refused to disclose SR Data, the reasons relied upon to refuse to disclose the SR Data, including any provision of the CDR Rules or Data Standards.

Dispute resolution provisions

- 8.23 Proposed Rule 1.26 provides that where a Retail Data Holder requests relevant information from AEMO in relation to a CDR Consumer complaint or dispute with the Retail Data Holder in relation to an SR Data Request, AEMO must provide the information to the extent that it is reasonable to do so.
- 8.24 Additionally, the proposed introduction of Part 5 of Schedule 4 to the CDR Rules will set out specific internal and external dispute resolution requirements in respect of the energy sector.



Part E ANALYSIS OF RISKS

9. Introduction

- 9.1 This **Part E** contains our analysis of the risks that we have identified as a result of the proposed amendments to the CDR Rules.
- 9.2 For convenience, we have grouped the identified issues under the following headings:
- 9.2.1 the role and obligations of AEMO;
 - 9.2.2 the roles and obligations of Retail Data Holders;
 - 9.2.3 risks associated with the scope of energy sector data;
 - 9.2.4 Direct to Consumer Requests; and
 - 9.2.5 individuals who are not CDR Consumers making the Consumer Data Request being the subject of CDR Data.
- 9.3 We have described and considered the potential high level privacy impacts we have identified in the tables below, together with some of the key existing mitigation strategies that are already included in the legislative framework underpinning the CDR regime, or are intended to be included in the proposed amendments to the CDR Rules. Where relevant, we have also included our high-level analysis of, and preliminary recommendations to mitigate, any identified gaps.

10. General impacts

- 10.1 As raised in previous PIA Update reports, it will be very important that all entities participating in the CDR regime (such as Retail Data Holders and AEMO) understand, and take steps to action, their obligations under the legislative framework. In addition, it will be important that CDR Consumers understand their rights under the CDR regime.
- 10.2 Accordingly, we **recommend** that Treasury arrange for detailed, comprehensive and clear guidance about the intended application of the CDR Rules, as amended by the proposed changes, to be issued. We suggest that specific guidance could be developed to assist:
- 10.2.1 CDR Consumers;
 - 10.2.2 AEMO; and
 - 10.2.3 Retail Data Holders.



11. Risks associated with the role and obligations of AEMO

Risks associated with the role and obligations of AEMO			
No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendations
1.	<p>AEMO may receive personal information from a Retail Data Holder in connection with a Consumer Data Request, which results in AEMO holding CDR Data from which a CDR Consumer could be identified</p> <p>This is because it is possible that a Retail Data Holder may provide AEMO with information about the CDR Consumer in the course of assisting a Retail Data Holder to fulfil a Consumer Data Request, or respond to a CDR Consumer’s complaint or dispute.</p> <p>Many of the proposed amendments to the CDR Rules (and CDR Regulations) have been drafted on the basis that AEMO will not hold CDR Data from which a CDR Consumer could be identified.</p>	<p>It is intended that the Data Standards will provide that Retail Data Holders must not provide any personal information to AEMO.</p> <p>If AEMO is required to provide assistance after providing CDR Data to a Retail Data Holder in fulfilment of a Consumer Data Request (e.g. by assisting a Retail Data Holder to respond to a CDR Consumer’s complaint or dispute), it is intended that a ‘transaction identifier’ will be used to enable AEMO to identify the relevant CDR Data (i.e. AEMO will not require a CDR Consumer’s personal information).</p> <p>If AEMO receives personal information from a Retail Data Holder, AEMO will need to comply with the Privacy Act and any relevant obligations under the National Energy Legislation in respect of that personal information.</p>	<p>In the unlikely event that AEMO receives personal information about a CDR Consumer from a Retail Data Holder (for example, when a Retail Data Holder is seeking assistance to resolve a complaint or dispute under the CDR regime), it is arguable that AEMO may, depending on the nature of the information, then be able to identify one or more CDR Consumers for the data that AEMO holds. If this risk eventuates, AEMO may hold CDR Data from which a CDR Consumer could be identified, but it would not be subject to all of the obligations of a Data Holder.</p> <p>Recommendation: <i>We recommend that, before commencement of the amendments to the CDR Rules, Treasury confirm that the Data Standards do (or will) prohibit Retail Data Holders from disclosing information to AEMO about CDR Consumers if that information would allow AEMO to identify one or more CDR Consumers for the data held by AEMO.</i></p>



Risks associated with the role and obligations of AEMO			
No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendations
		AEMO will be subject to many (although not all) of the Privacy Safeguards under proposed amendments to the CDR Regulations.	
2.	<p>CDR Consumers may not be made aware of the role of AEMO in the CDR regime</p> <p>Given the complexity of the CDR regime, and the unique role of AEMO in the energy sector, CDR Consumers may not understand the involvement of AEMO when giving their consents and authorisations.</p>	<p>Privacy Safeguard 1 requires, amongst other things, CDR entities who are bound by the Privacy Safeguards (including Accredited Data Recipients and Retail Data Holders, but not AEMO if the proposed amendments to the CDR Regulations are made) to handle CDR Data in an open and transparent manner. For example, these CDR entities will have to reflect how AEMO Data is handled in their CDR Policies.</p> <p>The CDR regime has generally applicable protections relating to how consent and authorisation must be obtained from CDR Consumers, which will apply to consent and authorisations for handling of CDR Data in the energy sector.</p>	<p>While AEMO will be a Data Holder, it is proposed that it will not be subject to all of the obligations of a Data Holder and will not have any direct relationship with CDR Consumers in order to obtain authorisation to disclose CDR Data.</p> <p>The amendments to the CDR Rules introduce the concept of a Primary Data Holder (in the energy sector, the Retail Data Holder) collecting CDR Data from a Secondary Data Holder (in the energy sector, AEMO), before disclosing it to an Accredited Data Recipient in fulfilment of a Consumer Data Request.</p> <p>Before giving consent or authorisation, it would be privacy best-practice if CDR Consumers were made aware that if they provide a collection consent to an Accredited Person, or provide authorisation to a Retail Data Holder, where this will also involve the collection of relevant information from AEMO. We appreciate that, unless expressly specified in the consent and authorisations, CDR Consumers are unlikely to know about AEMO (or realise that AEMO has a role in the fulfilment of Consumer Data Requests).</p> <p>The OAIC is of a similar view, noting that it has recommended that:</p> <p><i>‘Treasury make Rules that require retailers to provide additional information regarding their interactions with AEMO in their CDR policy and through the relevant</i></p>



Risks associated with the role and obligations of AEMO			
No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendations
			<p><i>authentication, authorisation and notification processes’.</i></p> <p>However, we appreciate that this will have to be balanced against the risk that CDR Consumers may experience ‘information overload’ if they are provided with too many notifications.</p> <p>Recommendation: <i>We recommend that Treasury consider whether it would be appropriate to make CDR Consumers aware of the involvement of AEMO in respect of the fulfilment of Consumer Data Requests, or whether this would risk ‘information overload’ for CDR Consumers or be otherwise unnecessary. This may involve the Data Standards Body undertaking consumer research as required.</i></p>



3. AEMO will not be required to disclose data to Retail Data Holders on request

AEMO will be authorised, but not required, to provide data to Retail Data Holders on request (i.e. because a Retail Data Holder is seeking to fulfil a Consumer Data Request). There is therefore a potential privacy risk that CDR Consumers may not be able to access all relevant CDR Data.

It is proposed that the CDR Rules will authorise, but not require, AEMO to disclose data to Retail Data Holders on request.

Additionally, it is not clear whether there are any limitations on when AEMO may decide not to respond to a Retail Data Holder’s request for CDR Data.

We understand that this issue arises because the CC Act currently allows the CDR Rules to authorise the disclosure of CDR Data from a Secondary Data Holder (e.g. AEMO) to a Primary Data Holder in response to a Consumer Data Request, but cannot *require* this. This may be because, at the time of the introduction of the CDR regime, the P2P model was not contemplated.

This represents a privacy risk because CDR Consumers will not necessarily be able to access and control their CDR Data through the CDR regime.

Recommendation: *While the risks may be low for the energy sector in circumstances where there is only one Secondary Data Holder (AEMO), we recommend that Treasury consider whether further amendments to the CC Act should be proposed in future, if the P2P model is to be applied to other designated sectors. For example, changes could be made so that a Secondary Data Holder is required to disclose CDR Data it holds to a Primary Data Holder in response to a valid Consumer Data Request. However, we do appreciate that there may be circumstances where it is reasonable for a Secondary Data Holder to refuse to provide the requested data, and the benefits of the refusal outweigh the privacy benefits for CDR Consumers in being provided with access to the CDR Data. We recommend that, if such circumstances are identified, these be set out in the CDR Rules, with guidance*



Risks associated with the role and obligations of AEMO			
No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendations
			<i>provided (for example, in the Data Standards) that clearly explains the scope of the exemption.</i>



Risks associated with the role and obligations of AEMO

No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendations
4.	<p>AEMO may disclose data to a retailer that is not a Retail Data Holder for the purposes of the CDR regime</p> <p>Because AEMO will not use the Accreditation Register to establish whether a retailer is a Retail Data Holder for the purposes of the CDR regime, it is possible that AEMO could disclose CDR Data to a retailer that does not meet the relevant definitions to be classified as a Retail Data Holder (i.e. AEMO could disclose data outside of the CDR regime).</p>	<p>AEMO will rely on its established systems and the information security profile already in place between AEMO and retailers to determine whether a retailer is a Retail Data Holder for the purposes of the CDR regime, such that it can accept and fulfil Consumer Data Requests. AEMO will only be able to provide CDR Data to a Retail Data Holder in response to a request from a Retail Data Holder (i.e. AEMO will not be able to provide CDR Data to a Retail Data Holder without first receiving a technical request).</p> <p>Given the time and cost involved, it is likely that only retailers that are Retail Data Holders will have built the necessary infrastructure to make a request to AEMO in accordance with the Data Standards.</p> <p>The Retail Data Holder will still be obliged to use the Accreditation Register to check the accreditation of an Accredited Data Recipient before it discloses the CDR Data (including that received from AEMO) to that Accredited Data Recipient.</p>	<p>In our view, given the existing mitigations, there is only a low risk that AEMO will provide CDR Data in response to a request made by an entity that is not a Retail Data Holder.</p> <p>However, in the unlikely event that AEMO were to disclose CDR Data (in response to a request) to an entity that is not a Retail Data Holder for the purposes of the CDR regime (noting the absence of a requirement to use the Accreditation Register to identify registered Retail Data Holders), then the Privacy Safeguards would not apply to that entity. It is possible that that entity may not be bound by other privacy legislation. This means that a CDR Consumer's CDR Data will not be protected in accordance with the Privacy Safeguards (and possibly, other privacy legislation). In other words, CDR Consumers would be afforded fewer (or, possibly, no) privacy protections in respect of the relevant data that was disclosed. However, we understand that any entity to which AEMO is likely to disclose any data is likely to also be a registered participant in the National Electricity Market, who would be bound by confidentiality obligations under Rule 8.6.1 of the National Electricity Rules.</p> <p>Recommendation: <i>We recommend that Treasury satisfy itself that AEMO's existing mechanisms will enable it to determine whether a retailer is a Retail Data Holder for the purposes of the CDR regime. In particular, we recommend that Treasury satisfy itself that AEMO will have access to real-time information about whether, at any given point in time, a retailer is a Retail Data Holder for the purposes of the CDR regime.</i></p>



Risks associated with the role and obligations of AEMO

No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendations
5.	<p>AEMO may, in the future, hold CDR Data from which a CDR Consumer could be identified by AEMO</p> <p>As discussed above, many of the proposed amendments to the CDR Rules (and CDR Regulations) have been drafted on the basis that AEMO will not hold CDR Data from which a CDR Consumer could be identified by AEMO.</p> <p>However, there is a risk that regulatory or other changes may occur in the future, so that AEMO does hold CDR Data from which a CDR Consumer could be identified by AEMO.</p>	<p>It is proposed that AEMO will be required to comply with all of the Privacy Safeguards except for Privacy Safeguards 1, 11 and 13. In circumstances where AEMO does not hold CDR Data from which a CDR Consumer could be identified, and is reliant upon other participants in the National Energy Market for the quality of the data that it does hold, these exceptions seem appropriate.</p> <p>Similarly, it is proposed that AEMO will not be required under Privacy Safeguard 10 to notify the disclosure of CDR data by AEMO to a Retail Data Holder. Again, this seems appropriate given AEMO will not have any direct relationship with CDR Consumers.</p>	<p>We note that the energy sector operates on the basis that whilst AEMO does hold some personal information in connection with retailers (i.e. the contact details of individuals working for particular retailers), AEMO does not hold identifiable information about, nor does it interact directly with, consumers. In other words, while AEMO does hold a significant amount of data given its role as the energy market operator, AEMO does not hold information from which a CDR Consumer could be identified by AEMO. We understand that this is a long-standing position in the energy sector and it is not anticipated that this is likely to change.</p> <p>While we appreciate that AEMO does not currently hold CDR Data from which a CDR Consumer could be identified by AEMO, and consider that the proposed exemptions to the Privacy Safeguards seem appropriate in that context, we consider that there is still a risk that in the future AEMO’s data holdings could change (either as a result of regulatory changes, or otherwise), such that it does hold CDR Data from which it could identify a CDR Consumer. Although, we understand that Treasury views this as a low risk, given that there are currently no plans to change AEMO’s data holdings.</p> <p>If this risk eventuates and the proposed amendments to the CDR Rules have commenced, AEMO would still not be subject to all of the obligations of a Data Holder. If the CDR Consumer can be identified by AEMO, it is more difficult to see why some of the ‘usual’ obligations of a Data Holder under the CDR Regime should not apply.</p> <p>This risk has also been identified by the OAIC, who has recommended that:</p>



Risks associated with the role and obligations of AEMO			
No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendations
			<p><i>'the PIA explicitly address whether AEMO will hold any CDR data for which there are one or more CDR consumers under the new peer-to-peer arrangements. Further, that the PIA consider whether any additional protections are required to ensure that the new energy data flows in CDR do not result in AEMO handling any CDR data for which there is a consumer.'</i></p> <p>Recommendation: We recommend that:</p> <ul style="list-style-type: none"> • <i>Treasury consider whether it is appropriate to build flexibility into the CDR Rules so that all of the obligations on Data Holders, including the obligation to comply with all of the Privacy Safeguards, will automatically apply to AEMO if it holds CDR Data from which it could identify a CDR Consumer; and/or</i> • <i>AEMO be required to:</i> <ul style="list-style-type: none"> ○ <i>implement processes and systems to be able to identify if it does become the holder of CDR Data from which a CDR Consumer could be identified by AEMO; and</i> ○ <i>notify the CDR regulators if this occurs, so that appropriate steps can be taken as a result, if required.</i>



12. Risks associated with the role and obligations of Retail Data Holders

Risks associated with the role and obligations of Retail Data Holders			
No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendations
6.	<p>Retail Data Holders may collect unsolicited data from AEMO</p> <p>There is a risk that Retail Data Holders may collect unsolicited data from AEMO – for example, if AEMO was to provide data about the “wrong” CDR Consumer.</p>	<p>The proposed amendments to the CDR Rules will require Data Holders (for example, Retail Data Holders) to destroy SR Data as soon as practicable if it was purportedly collected under the CDR Rules (but not as the result of seeking to collect that SR Data) and is not required to be retained by, or under, an Australian law or court/tribunal order (see proposed Rule 1.25).</p> <p>In addition, APP 4 in the Privacy Act will apply to the Retail Data Holder if they are an APP entity.</p> <p>We assume that AEMO, given its role under the National Energy Legislation, will have procedures in place to reduce the risks of providing unsolicited data to a Retail Data Holder.</p>	<p>We consider that the proposed amendments to the CDR Rules that will require Retail Data Holders to destroy unsolicited SR Data (subject to the exception described above) will mitigate the risks associated with Retail Data Holders potentially collecting unsolicited data from AEMO.</p>
7.	<p>Retail Data Holders not required to keep records regarding their dealings with AEMO</p> <p>If Retail Data Holders are not required to keep records about</p>	<p>Proposed rule 9.3(1)(ca) provides that Retail Data Holders must keep records regarding their dealings with AEMO.</p>	<p>We consider that the proposed amendments to the CDR Rules will mitigate this risk.</p>



Risks associated with the role and obligations of Retail Data Holders			
No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendations
	<p>their dealings with AEMO, this raises a risk for CDR Consumers that may make a complaint – i.e. the Retail Data Holder may not necessarily hold all of the relevant information necessary to resolve or consider the complaint.</p>		



13. Risks associated with the scope of energy sector data

Risks associated with the scope of energy sector data			
No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendation
8.	<p>Approach to historical metering data</p> <p>AEMO may release CDR Data that relates to a consumer other than the CDR Consumer making a Consumer Data Request</p> <p>If AEMO does release historical metering data, this may disclose some information about a third party individual’s energy usage over a particular period.</p>	<p>The proposed amendments to the CDR Rules specify that only data that ‘relates to a time at which an account holder for the relevant account was associated with the premises to which the request relates’ is within the definition of Required Consumer Data or Voluntary Consumer Data (see proposed Rule 3.2). This will mean that AEMO and Retail Data Holders are only authorised to disclose CDR Data about a CDR Consumer for the period the consumer was associated with the relevant premises.</p>	<p>We consider it is privacy-enhancing for CDR Consumers to be able to access CDR Data regarding their premises for the time they are associated with the relevant premises.</p> <p>However, the CDR Rules do not indicate how a Retail Data Holder or AEMO will be able to establish when a CDR Consumer first became associated with the relevant premises (the Retail Data Holder will only know this information from the date the CDR Consumer became an account holder with that retailer (for the relevant premises) and AEMO does not currently hold information that would enable it to determine when a customer associated with an NMI (being a number used to identify every electricity network connection point in Australia) changes).</p> <p>We understand that, in practice, it is intended that AEMO will only release CDR Data where the Retail Data Holder is able to confirm that the relevant CDR Consumer is the account holder for the relevant premises (i.e. from the time the CDR Consumer became an account holder with that Retail Data Holder in respect of those premises). In our view, if there are appropriate practical mechanisms in place, this should sufficiently mitigate the risk.</p>
9.	<p>AEMO and Retail Data Holders have modified PS obligations in respect of AEMO Data</p>		<p>We understand that the amendments to the CDR Regulations will effectively exempt AEMO from PS 1, 10, 11 and 13 in relation to AEMO Data. In addition, the amendments to the CDR Regulations will clarify that if Retail Data Holders receive CDR Data from AEMO, then they must comply with PS 1 and 10 in respect of that data. Further, the proposed amendments to the CDR Rules will mean that Retail Data Holders, if they receive a request for correction of</p>



Risks associated with the scope of energy sector data			
No.	Potential Privacy Risk	Existing mitigation strategies	Gap analysis and Recommendation
			<p>AEMO Data under PS 13, must comply with the modified requirements (see proposed Rule 6.1(2) of Schedule 4).</p> <p>The OAIC has suggested that Retail Data Holders should be subject to modified PS 11 obligations in respect of AEMO Data – i.e. that Retail Data Holders should be required to take reasonable steps to ensure that the AEMO Data they are disclosing is accurate.</p> <p>While we appreciate that there is a risk that a Retail Data Holder could disclose incorrect or incomplete AEMO Data to an Accredited Data Recipient, we do not consider that there are any reasonable steps that Retail Data Holders could take to prevent this. This is because:</p> <ul style="list-style-type: none"> • AEMO Data is comprised of information that has already been reported by retailers and other market participants to AEMO; and • Retail Data Holders have no oversight of AEMO’s data holdings and therefore would not be able to determine whether AEMO Data is correct and complete. <p>On this basis, and given the limited interaction between AEMO and CDR Consumers and AEMO’s existing obligations under the National Electricity Law, we do not consider that the proposed amendments will have a significant privacy impact for CDR Consumers.</p>



14. Impact of CDR Consumers in the energy sector being unable to make Direct to Consumer Requests

Impact of CDR Consumers in the energy sectors being unable to make Direct to Consumer Requests			
No.	Risk	Existing mitigation strategies	Gap analysis and Recommendation
10.	CDR Consumers in the energy sector will not be able to make Direct to Consumer Requests	We understand that in the energy sector, CDR Consumers are already able to directly access much of their energy data under the National Electricity Framework.	<p>While we appreciate that CDR Consumers can access much of their energy data directly from Retail Data Holders (and other retailers and distributors), we have not analysed whether CDR Consumers can access all of their CDR Data through these mechanisms, or whether they can access the CDR Data in a suitable form. In other words, there may be a gap between the data that CDR Consumers can currently access, and the CDR Data that CDR Consumers could access if they could make Direct to Consumer Requests. This means that CDR Consumers may not be able to control all of their CDR Data through the CDR regime, or may not be able to access all of their CDR Data in an appropriate form.</p> <p>We appreciate that further consultation with the energy sector would be required in respect of the potential introduction of Direct to Consumer Requests.</p> <p>Recommendation: <i>We recommend that, as part of further consideration of this issue, a detailed analysis be undertaken to determine the differences (if any) in the data that CDR Consumers can currently access under existing mechanisms, and the CDR Data that CDR Consumers would be able to access if they could make Direct to Consumer Requests. This analysis would assist all parties to understand the potential benefits for CDR Consumers in being able to make Direct to Consumer requests.</i></p>

15. **Individuals, who are not the CDR Consumer making the Consumer Data Request, being the subject of CDR Data**

Individuals, who are not the CDR Consumer making the Consumer Data Request, being the subject of CDR Data			
No.	Risk	Existing mitigation strategies	Gap analysis and Recommendation
11.	Individuals who are not CDR Consumers may be the subject of CDR Data and exposed to greater privacy risks in respect of the energy sector	<p>Rule 4.12(3)(b) of the CDR Rules provides that, subject to Rule 4.12(4), an Accredited Person must not ask for a consent for using CDR Data, including by aggregating the data, for the purposes of:</p> <ul style="list-style-type: none"> • identifying; • compiling insights in relation to; or • building a profile in relation to, <p>an identifiable individual who is not the CDR Consumer who made the Consumer Data Request.</p>	<p>The OAIC has suggested that, in the energy sector (as opposed to the banking sector), there may be a greater risk that CDR Data will contain sensitive information about individuals that are not the CDR Consumer who has made or authorised a Consumer Data Request.</p> <p>Accordingly, the OAIC has recommended that Treasury consider:</p> <p><i>‘whether further enhancements (whether to Rule 4.12(3)(b), or in the form of additional new rules) are required to mitigate against the privacy risks that may arise for non-consumers who are the subject of CDR energy data’.</i></p> <p>We appreciate that CDR Data in the energy sector may include information about, for example, the electricity usage of an individual other than the CDR Consumer who made the Consumer Data Request (e.g. a landlord who is responsible for paying an electricity bill for his rental property, may request CDR Data about the account, which would disclose the energy habits of the tenants).</p> <p>We note that the Original PIA Report considered the issue of CDR Data containing information about third party individuals who are not the CDR Consumer making the Consumer Data Request. We consider that the risks raised in the Original PIA Report apply</p>



Individuals, who are not the CDR Consumer making the Consumer Data Request, being the subject of CDR Data			
No.	Risk	Existing mitigation strategies	Gap analysis and Recommendation
			<p>equally to the energy sector, but do not consider that there is any magnified risk in the energy sector.</p> <p>On this basis, we do not consider that any further amendments to the CDR Rules are required, but note that Treasury may wish to consider publishing information explaining how it has balanced the competing privacy interests of CDR Consumers and third party individuals (as it did in its response to Recommendation 7 in the Original PIA Report).</p>

Part F GLOSSARY

Term	Meaning
ACCC	means the Australian Competition and Consumer Commission.
AEMO	means the Australian Energy Market Operator Limited.
Accredited Data Recipient	has the meaning given by section 56AK of the CC Act.
Accredited Person	means a person who holds an accreditation under section 56CA(1) of the CC Act.
Australian Privacy Principles (APPs)	means the Australian Privacy Principles at Schedule 1 to the Privacy Act.
CC Act	means the <i>Competition and Consumer Act 2010</i> (Cth).
CDR Consumer(s)	has the meaning given by section 56AI(3) of the CC Act.
CDR Data	has the meaning given by section 56AI(1) of the CC Act.
CDR Regulations	means the <i>Competition and Consumer Regulations 2010</i> (Cth).
CDR Rules	means the <i>Competition and Consumer (Consumer Data Right) Rules 2020</i> .
Consumer Dashboard	(a) in relation to an Accredited Person, has the meaning given by Rule 1.14 of the CDR Rules; or (b) in relation to a Data Holder, has the meaning given by Rule 1.15 of the CDR Rules.
Consumer Data Request	means a request made by a CDR Consumer, or by an Accredited Data Recipient on behalf of a CDR Consumer, to a Data Holder to obtain CDR Data about a CDR Consumer.
Data Holder(s)	has the meaning given by section 56AJ of the CC Act.
Data Standards	means the data standards made under section 56FA of the CC Act.
DER	means the distribution energy resources.
Minister	means the Minister for Superannuation, Financial Services and the Digital Economy.
NMI	means the national metering identifier.
OAIC	means the Office of the Australian Information Commissioner.
Original CDR PIA report	means the Privacy Impact Assessment report in relation to the Consumer Data Right Regime published on 11 December 2019.
P2P	means the Peer-to-Peer model which will apply in the energy sector and other designated sectors.



Maddocks

PIA Update reports	means the previous privacy impact update processes undertaken by the ACCC to analyse the impact of any proposed amendments to the CDR Rules.
PIA Update 3 Report	means this the third updated privacy impact report prepared by Maddocks.
PIA Update 4 Report	means this the fourth updated privacy impact report prepared by Maddocks.
Primary Data Holder	in relation to SR Data and a particular designated sector, means the Data Holder specified in the sector Schedule as the Primary Data Holder for the SR data.
Privacy Act	means the <i>Privacy Act 1988</i> (Cth).
Privacy Safeguards	means the provisions in Subdivision B to F of Division 5 of Part IVD of the CC Act.
Retail Data Holders	means the Primary Data Holders in the energy sector.
Secondary Data Holder	in relation to SR Data and a particular designated sector, means the Data Holder specified in the sector Schedule as the Secondary Data Holder for the SR Data.
SR Data	means shared responsibility data, which has the meaning set out in the relevant sector-specific schedule to the CDR Rules.
Treasury	means the Department of the Treasury.

Part G LIST OF SUBMISSIONS

We reviewed submissions from the following entities who submitted a response to Treasury's call for submissions on an exposure draft of the proposed amendments to the CDR Rules. For completeness, Maddocks also considered seven additional submissions on a confidential basis.

1. Australian Energy Council
2. Australian Energy Market Operator
3. AGL Energy Limited
4. Alinta Energy
5. Energy Consumers Australia
6. Energy Security Board
7. Momentum
8. Office of the Australian Information Commissioner
9. Public Interest Advocacy Centre
10. PwC Australia
11. Telstra