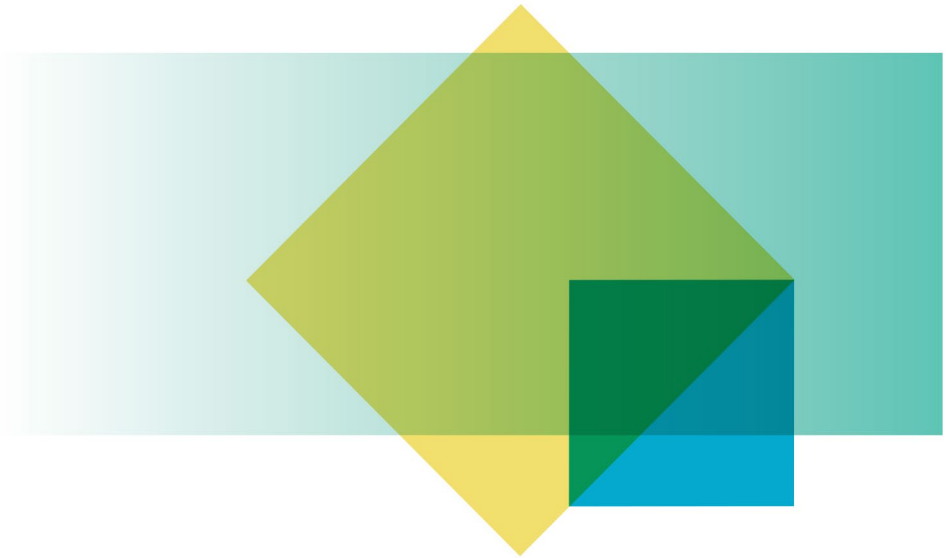
Australian Government

Office of the Australian Information Commissioner

OAIC Submission to the CDR Energy Rules Framework

Submission by the Office of the Australian Information Commissioner



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

31 August 2020

OAIC

Contents

Introduction 2

Recommendations 3

About the OAIC and our role in the CDR system 5

Comments on specific issues raised in the Framework 5

- Role of AEMO in the CDR system 5
- Clarity on AEMO's role needed to inform privacy-related Rules 6
- Rules relating to the privacy safeguards 7
- Unrestricted accreditation 10
- Tiered accreditation 11
- Interaction between the Rules and data standards 13
- Dashboards 14
- Approach to 'eligible' CDR consumers in the energy sector 15
- Authentication 19
- Implementation matters 20

Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Energy Rules Framework Consultation Paper (Framework) by the Australian Competition and Consumer Commission (ACCC). The Framework sets out the ACCC's proposed approach on how the Consumer Data Right (CDR) Rules will apply to the energy sector, and explores matters which may require specific sectoral rules for energy or amendments to the *Competition and Consumer (Consumer Data Right) Rules 2020* (existing Rules).

In particular, the Framework explores accommodating the Australian Energy Market Operator (AEMO) Gateway model, options for the authentication of energy consumers, having a single data holder consumer dashboard and the scope of the definition of 'eligible CDR consumer'. It also considers how tiered accreditation should be facilitated across the CDR, including the appropriateness of introducing a lower tier of accreditation for accredited data recipients (ADRs) who are seeking to receive energy CDR data only.

By way of overall comment, the OAIC is broadly supportive of the positions set out in the Framework. The OAIC agrees that there are matters unique to the energy sector that may need to be addressed in energy-specific Rules, including data flow arrangements to facilitate the AEMO gateway model and pre-existing practices in the energy sector (such as information security and internal dispute resolution processes).[1]

At the same time, the OAIC would recommend maintaining consistency with the existing Rules wherever possible, unless there is a compelling policy or privacy-enhancing reason to particularise rules for the energy sector. The existing Rules have been developed to reflect the sensitive nature of (all types of) CDR data, prevent any misuse of the data, and build consumer trust in the CDR system. It is critical that there is a consistent, high standard of privacy protection and accountability for CDR participants, regardless of the CDR sector with which they engage.

The existing Rules have also been designed to be sector-neutral, and to realise the broader CDR policy objective of having an economy-wide system which promotes interoperability within and across sectors. Maintaining consistency with the existing Rules as far as possible will also reduce complexity for participants and consumers.

On a separate note, the OAIC would caution against any dilution of the existing privacy protections under the Rules, on the basis of the assumption that energy data is less sensitive than banking data.[2] As outlined further in this submission, a more considered analysis of the sensitivity of energy data is required before particularisation on this basis should be considered. Energy data can, like banking data, reveal granular insights about many aspects of an individual's life. For example, emerging technologies, such as smart meters and sensors are increasingly used in the energy sector to improve energy efficiency. Such devices make it easier to analyse consumption patterns, identify the use of specific appliances in a household, and track energy usage, which can be used to profile and extract insights into the movements, lifestyle and interests of occupants.[3] Further, as CDR is

[1] See sections 2 and 4.5 of the Framework.

[2] We note that the Supplementary Privacy Impact Assessment for the energy sector found there was consensus amongst stakeholders that energy data does not generally have the same sensitivities as banking data: KPMG, *Consumer Data Right in the Energy Sector*, Supplementary Privacy Impact Assessment for the Commonwealth Department of Treasury, 25 May 2020, section 7.5.

[3] Examples as suggested in the Utilligent submission to the Treasury's consultation on the priority energy data sets include what time occupants wake up and/or go to sleep, when all occupants typically leave the house for the day, bathing and cooking patterns and when occupants water their garden or watch television.

rolled out across the economy and data sets can be combined, richer and more granular insights may be derived about individual consumers from CDR data, meaning the overall privacy risks for consumers may increase.[4] More generally, considerations as to the sensitivity of a data set should have regard to the broader context of data use and amalgamation, in which data analytics and other data aggregation activities may be used to generate sophisticated insights in relation to and between data sets.

Finally, the OAIC also notes that many significant privacy considerations, including the data handling limitations that will apply to the designated gateway, data holders and ADRs, have not been outlined or explored in the Framework in detail. Further, where significant privacy issues are explored in the Framework (for example the energy-specific Rules that may need to be made in relation to the privacy safeguards), these are outlined at a high level. We appreciate that this is because the technical design and function of the AEMO gateway model has not been finalised, and that the ACCC intends to review these matters at a later point in time. However, the OAIC recommends that these privacy matters are considered as early as possible as part of the design of the AEMO gateway model, to ensure that they are fully integrated in the CDR framework for the energy sector.

In this submission, the OAIC provides further comments and recommendations on specific issues raised in the Framework. We are available to discuss any aspect of our submission further with the ACCC, and more generally to assist with any aspect of the development of the Rules for the energy sector.

Recommendations

1. To reduce the risks associated with additional or unnecessary collection and handling of data, the OAIC strongly supports the adoption of the proposed 'conduit' model for AEMO in its capacity as the designated gateway, which would mean AEMO would not store or hold any CDR data (or do so only on a limited basis).

2. The OAIC recommends that key privacy matters, such as the privacy and security settings for AEMO and the data handling limitations that should apply to each CDR entity, are considered as early as possible as part of the design of the AEMO gateway model, to ensure that they are fully integrated in the CDR framework for the energy sector. The OAIC further recommends that these matters be considered as part of the privacy impact assessment to be conducted in relation to the AEMO gateway's platform and systems.

3. The OAIC recommends that appropriate data handling limitations be placed upon AEMO through the Rules, as are commensurate with its role in the CDR system.

4. The OAIC recommends that a further review of the energy-specific Rules required under or in relation to the privacy safeguards be undertaken as soon as practicable after the design and functionality of the gateway becomes clearer. The OAIC offers its expertise to the ACCC in the conduct of this review.

---

[4] The OAIC provided a public submission in response to the Treasury's consultation on the priority energy data sets in which we outlined the privacy risks associated with energy data sets and the combining of energy data with banking data as CDR is rolled out across the economy.

By way of example, according to the Australian Retail Credit Association's submission to the Treasury's consultation on the priority energy data sets, energy data could also support use cases of banking data related to lending – for example energy billing data could provide additional insights to supplement banking transaction data, such as the value and due date of energy bills.

5. The OAIC recommends that any departure from the stringent information security requirements in Schedule 2 of the existing Rules be considered carefully in light of the specific privacy and security risks associated with the gateway function. Where AEMO will collect and hold CDR data in its gateway capacity, the OAIC considers it would be appropriate for the information security requirements in Schedule 2 of the existing Rules (or equivalent) to apply to the gateway.

6. The OAIC recommends that any changes to accreditation requirements should be carefully tailored to mitigate the risks posed by the specific data handling activities of the relevant entities, and in a way that ensures the privacy and security risks are managed consistently across the scheme and the overall integrity of the CDR system is maintained.

   In particular, the OAIC recommends that accredited persons at all tier levels should remain subject to the Privacy Act (see s 6E(1D)), as well as the strong consent, notification and other transparency requirements that currently apply to accredited persons in the CDR.

7. The OAIC recommends that the ACCC gather and consider evidence about the potential privacy risks for consumers from the handling of their energy data, as part of their exploration of whether a lower tier of accreditation to access energy data is appropriate. The OAIC further recommends this exercise occur ahead of CDR being launched in the energy sector.

8. The OAIC recommends that the ACCC consider a broad range of strategies for mitigating privacy risks posed by tiered accreditation. By way of example, it may be appropriate to limit the format in which a person accredited at a lower level may receive CDR data (i.e. to a modified, lower-risk format), or provide that the person can only use CDR data for specific purposes that have been subject to careful consideration, and deemed to be lower-risk.

9. The OAIC recommends that the ACCC adopt 'Option 1' for the provision of data holder consumer dashboards in the energy sector. More generally, the OAIC considers that any process set out in the Rules for providing the data holder consumer dashboard must be supported by robust privacy and security settings, including appropriate data handling limitations on the dashboard provider and any third party service providers engaged by the dashboard provider.

10. The OAIC recommends the ACCC consider further how including consumers with offline accounts will impact on obligations of data holders and ADRs in the existing Rules, and how that arrangement should affect the development of relevant Rules for the designated gateway. Adjustments or additional requirements may need to be made to the Rules in light of this review. For example, the OAIC would recommend that appropriate changes be made to the information security controls in Schedule 2 of the existing Rules to enable offline participation, and to ensure that privacy protections are not diluted for those using offline mediums to engage with the CDR system.

11. The OAIC supports the ACCC's preference for authentication Model 1 and recommends that the ACCC adopt this model for consumers in the energy sector. Given that Model 1 may encompass offline authentication processes, the OAIC further recommends the ACCC ensure the same high level of security that exists for online authentication can be achieved by offline authentication processes.

About the OAIC and our role in the CDR system

The OAIC is Australia's independent regulator for privacy and freedom of information. The OAIC co-regulates the CDR scheme together with the ACCC. The OAIC enforces the privacy safeguards (and related Rules) and advises the ACCC and Data Standards Body on the privacy implications of the CDR Rules and data standards. The OAIC is also responsible for undertaking strategic enforcement in relation to the protection of privacy and confidentiality, as well as investigating individual and small business consumer complaints regarding the handling of their CDR data.

Our goal in regulating the privacy aspects of the CDR system is to ensure that the system has a robust data protection and privacy framework, and effective accountability mechanisms to ensure consumers are protected.

Comments on specific issues raised in the Framework

Role of AEMO in the CDR system

The Australian Energy Markets Operator (AEMO) has been designated as a gateway to facilitate the transfer of certain types of CDR data from data holders to accredited persons in the energy sector.[5] As AEMO has also been designated as a data holder for specific types of CDR data,[6] AEMO will only be a gateway for CDR data held by or on behalf of retailer data holders.

As outlined in section 4.1.2 of the Framework, the ACCC's preliminary view on the role of the AEMO gateway is that it will function as a 'conduit' for data provided by retailer data holders to accredited persons – AEMO will not hold or store the data it receives from data holders in its gateway capacity except where necessary to facilitate its gateway function.

The OAIC strongly supports the proposed 'conduit' model for the AEMO gateway, meaning AEMO would not store or hold any CDR data in its gateway capacity (or would do so only on a very limited basis, to the extent necessary to facilitate its gateway function). This model is preferable as it will reduce the privacy risks associated with additional or unnecessary collection and handling of data.

Recommendation 1

To reduce the risks associated with additional or unnecessary collection and handling of data, the OAIC strongly supports the adoption of the proposed 'conduit' model for AEMO in its capacity as the designated gateway, which would mean AEMO would not store or hold any CDR data (or do so only on a limited basis).

[5] Section 6(4) of the *Consumer Data Right (Energy Sector) Designation 2020*.

[6] Section 6(2) of the *Consumer Data Right (Energy Sector) Designation 2020*.

Clarity on AEMO's role needed to inform privacy-related Rules

The OAIC understands from section 4.1 of the Framework that the details of the gateway's technical design and function in the CDR system are under active consideration by the ACCC. As a result, the ACCC's preliminary policy positions in section 4.1 on areas where Rules may be required to facilitate AEMO's role are high-level – the ACCC notes that 'additional requirements may be necessary pending [finalisation of] the gateway's technical design and function'.

As outlined below, the OAIC considers that the details of the gateway's technical design and function will be critical in determining the approach to many significant privacy matters in the Rules. Some of these privacy matters have not been explored in the Framework, while others have been outlined but at a high level only. The OAIC appreciates this is because the technical design and function of the gateway has not been settled, and that the ACCC intends to review some of these matters at a later point in time. However, the OAIC recommends that these privacy matters are considered as early as possible as part of the design of the gateway model, to ensure that they are fully integrated in the CDR framework for the energy sector.

The OAIC notes that the supplementary privacy impact assessment (PIA) for the energy sector recommended that a PIA be conducted on the AEMO gateway's proposed platform and systems, with involvement from AEMO, Treasury, ACCC, Data61 and the OAIC.[7] This recommendation was accepted.[8] The OAIC considers this PIA will assist the ACCC to comprehensively explore key privacy matters and that the privacy risks and mitigation strategies contained in that PIA will inform the energy-specific Rules that are required in light of AEMO's design and function.

The OAIC further understands from section 4.1.2 of the Framework that the ACCC intends to make Rules relating 'to the disclosure, collection, use, accuracy, storage, security and deletion of CDR data by the gateway'. We note that not all elements listed here may be relevant to AEMO, which will depend on the specific design and function of the gateway. For example, if AEMO will not hold or store CDR additional data,[9] it is possible that AEMO may not 'collect' CDR data within the meaning of the *Competition and Consumer Act* (if data is not collected for inclusion in a record).[10]

Recommendation 2

The OAIC recommends that key privacy matters, such as the privacy and security settings for AEMO and the data handling limitations that should apply to each CDR entity, are considered as early as possible as part of the design of the AEMO gateway model, to ensure that they are fully integrated in the CDR framework for the energy sector. The OAIC further recommends that these matters be considered as part of the privacy impact assessment to be conducted in relation to the AEMO gateway's platform and systems.

[7] KPMG, *Consumer Data Right in the Energy Sector*, Supplementary Privacy Impact Assessment for the Commonwealth Department of Treasury, 25 May 2020, Recommendation 2.

[8] See the Agency Response to the Consumer Data Right Energy Privacy Impact Assessment, 22 June 2020, p. 5.

[9] In its capacity as a designated gateway (AEMO is a data holder and therefore already holds certain types of CDR data).

[10] The OAIC would be pleased to discuss this further with the ACCC as the specifics of the data transfers under the gateway model become clearer.

Privacy and security settings for AEMO

The technical design and function of the gateway will determine the specific way in which AEMO will handle CDR data, and will therefore be critical in determining what privacy and security settings are appropriate for AEMO.

The Framework states in section 4.1.2 that the Rules should otherwise restrict AEMO from handling CDR data for which it is not a data holder, except where needed to support the transfer of CDR data to data holders. The OAIC strongly supports this and more broadly recommends that appropriate data handling limitations be placed upon AEMO through the Rules, as are commensurate with its role in the CDR system.

Recommendation 3

The OAIC recommends that appropriate data handling limitations be placed upon AEMO through the Rules, as are commensurate with its role in the CDR system.

Data handling limitations for CDR entities

The OAIC considers that the specific design and function of the gateway will be important in determining what requirements and adjustments to the existing Rules are needed to regulate information flows between the gateway, data holders and ADRs. This is because the technical design and function of the gateway will clarify these information flows, in particular, by confirming what data is required to be transferred between the CDR entities. This will inform what data handling limitations are appropriate to apply to the gateway, data holders and ADRs.

Privacy safeguards

As outlined in the following section, the OAIC considers that the technical design and function of the gateway will inform the details of the privacy safeguard-related Rules that are required for the energy sector.

Rules relating to the privacy safeguards

The privacy safeguards are legally binding statutory provisions, which ensure the security and integrity of the CDR system by setting out obligations in relation to the handling of CDR data for which there are one or more consumers.[11] The specific requirements for certain privacy safeguards are set out in the current version of the CDR Rules.

The Framework provides, in section 4.1.3.6, that the ACCC will 'likely conduct a final review of the privacy safeguards once appropriate decisions regarding the design and functionality of the gateway are finalised'. As noted in the previous section the OAIC considers that the technical design and function of the gateway will inform the details of the privacy safeguard-related Rules required for the energy sector. Consequently, the OAIC recommends this review be undertaken as soon as

[11] The privacy safeguards apply to CDR data for which there are one or more CDR consumers: s 56EB(1) of the Competition and Consumer Act. One requirement for CDR data to have a CDR consumer is that there needs to be at least one person who is identifiable, or reasonably identifiable, from the CDR data or from related information (see s 56AI(3)(c) of the Competition and Consumer Act).

practicable after the design and functionality of the gateway becomes clearer. The OAIC offers its expertise to the ACCC in the conduct of this review.

As outlined in section 4.1.3.6 of the Framework, the ACCC expects that the requirements placed on the gateway regarding the applicable privacy safeguards will be 'broadly consistent' with the existing privacy safeguard-related Rules in Part 7. The ACCC has, however, provided examples of privacy safeguard-related Rules that may need to specifically address the gateway (in section 4.1.1.2 of the Framework). The OAIC agrees with this analysis, and considers there are a number of additional instances in which energy-specific Rules may need to be made under or in relation to the privacy safeguards to reflect the role of the gateway and other industry-specific matters. These are outlined below.

The OAIC notes that it will review and update the CDR Privacy Safeguard Guidelines to address the need for guidance on any privacy safeguard-related Rules that are made in relation to the energy sector. We look forward to consulting with the ACCC and industry on these updates at the appropriate time.

Recommendation 4

The OAIC recommends that a further review of the energy-specific Rules required under or in relation to the privacy safeguards be undertaken as soon as practicable after the design and functionality of the gateway becomes clearer. The OAIC offers its expertise to the ACCC in the conduct of this review.

Privacy Safeguard 1 – transparency measures

Privacy Safeguard 1 requires designated gateways, data holders and ADRs to have a CDR policy about the management of CDR data.[12] To ensure consumers are informed about the role of the gateway in the collection and disclosure of their energy CDR data, the OAIC suggests the ACCC consider whether the Rules relating to Privacy Safeguard 1 should require ADRs and data holders to include information about the gateway's role (for example, notification that certain data sets will be transferred through the gateway) in their CDR policy.

The OAIC acknowledges that in considering these matters there is a need to balance consumer transparency with comprehension.

Privacy Safeguard 2 – anonymity and pseudonymity

Privacy Safeguard 2 requires an ADR to give a consumer the option of using a pseudonym, or not identifying themselves, when dealing with the ADR. These options may be offered by an ADR through a designated gateway.[13]

To give effect to this, the OAIC considers that Rules may need to be made in relation to the matters covered by Privacy Safeguard 2 for both ADRs and the gateway.

[12] Section 56ED(3) of the Competition and Consumer Act.

[13] Section 56EE(2) of the Competition and Consumer Act.

Privacy Safeguard 6 – use and disclosure of CDR data

Privacy Safeguard 6 provides that ADRs and designated gateways must not use or disclose CDR data unless authorised to do so under the Rules. The existing Rules made under Privacy Safeguard 6 are in relation to ADRs, and principally cover how ADRs are permitted to use and disclose CDR data to provide the consumer with the requested goods or services.[14]

The OAIC therefore considers that specific Rules would need to be developed under Privacy Safeguard 6 for the designated gateway.[15] These Rules would need to be different to the Rules that currently exist under Privacy Safeguard 6 for ADRs, to reflect AEMO's role as a 'conduit' for CDR data.

Privacy Safeguard 7 – direct marketing

Privacy Safeguard 7 provides that designated gateways must not use or disclose CDR data for direct marketing unless required or authorised under the CDR Rules.[16]

Given AEMO's role as a 'conduit' for CDR data, the OAIC considers that AEMO should not engage in direct marketing and would therefore not expect any Rules to be made under Privacy Safeguard 7 in relation to the designated gateway for the energy sector.

Privacy Safeguard 11 – disclosure of corrected CDR data

Privacy Safeguard 11 requires a data holder to disclose corrected CDR data to an ADR in certain circumstances.[17]

For the energy sector, the OAIC has assumed that corrected CDR data would need to pass through the AEMO gateway (as the gateway acts as a 'conduit' for the transfer of all CDR data between data holders and ADRs). On this basis, the OAIC considers that energy-specific Rules (and/or data standards) may be needed under Privacy Safeguard 11 to facilitate the disclosure of corrected CDR data from a data holder to an ADR.

Privacy Safeguard 12 – information security

Privacy Safeguard 12 requires ADRs and designated gateways to take the steps specified in the CDR Rules to protect CDR data from misuse, interference, loss, unauthorised access, modification or disclosure.[18] The relevant steps that ADRs must take are contained in Schedule 2 of the existing Rules.

As per section 4.1.3.4, the ACCC is seeking feedback on whether the information security controls that currently apply to ADRs should apply to the gateway, or whether the gateway should be required to comply with an external standard instead (such as the Australian Energy Sector Cyber Security Framework).

The OAIC understands that the specifics of the gateway's technical design and function are under consideration by the ACCC. The OAIC is therefore unable to comment at this stage on the specifics of what information security requirements might be appropriate. However, by way of general

---

[14] CDR Rule 7.5(1).

[15] Under section 56EI(2) of the Competition and Consumer Act.

[16] Section 56EJ(2) of the Competition and Consumer Act.

[17] Section 56EN(4) of the Competition and Consumer Act.

[18] Section 56EO(1) of the Competition and Consumer Act.

comment, the OAIC considers that information security requirements for the gateway need to be commensurate with AEMO's role and data handling activities (noting that AEMO may, in some potential models, hold or store CDR data).

Further, the OAIC would recommend that any departure from the stringent information security requirements in Schedule 2 of the existing Rules be considered carefully in light of the specific privacy and security risks associated with the gateway function. Where AEMO will hold or store CDR data, the OAIC considers it would be appropriate for information security requirements equivalent to those in Schedule 2 of the existing Rules to apply to the gateway.

Recommendation 5

The OAIC recommends that any departure from the stringent information security requirements in Schedule 2 of the existing Rules be considered carefully in light of the specific privacy and security risks associated with the gateway function. Where AEMO will hold or store CDR data in its gateway capacity, the OAIC considers it would be appropriate for the information security requirements in Schedule 2 of the existing Rules (or equivalent) to apply to the gateway.

Privacy Safeguard 13 – correction of CDR data

Privacy Safeguard 13 requires ADRs and data holders to take certain steps in response to a request from a consumer for the correction of their CDR data. [19]

The OAIC understands from section 3.3.1 of the Framework that processes for correction of certain energy data sets currently exist under national energy legislation, and that the Rules may need to allow for specific arrangements to recognise these existing processes.

The OAIC acknowledges these existing mechanisms and would support efforts to ensure consistency with these or otherwise ensure they are reflected in any energy-specific Rules that need to be developed.

Unrestricted accreditation

As outlined in section 4.7.1.1 of the Framework, there is currently one single 'unrestricted' level of accreditation in the CDR system. This 'unrestricted' level of accreditation enables an ADR to receive all CDR data within scope for the banking sector. The ACCC considers, as outlined in section 4.7.1.2, that persons accredited at this 'unrestricted' level should be able to receive all energy data, as well as banking data.

The OAIC supports the ACCC's intention to allow persons accredited at the 'unrestricted' level to receive all energy and banking CDR data within scope for those sectors. Persons accredited at the 'unrestricted' level are subject to stringent obligations, notably the requirement to demonstrate compliance with the information security requirements in Schedule 2 of the Rules before becoming accredited and on an ongoing basis thereafter.[20] Taking a CDR-wide approach to the 'unrestricted'

[19] Section 56EP of the Competition and Consumer Act.

[20] Part 2 of Schedule 1 to the CDR Rules. See also CDR Rule 5.12 for the obligations which apply to a person accredited at the 'unrestricted' level.

level of accreditation would also assist in facilitating interoperability both within and across sectors in the CDR.

Tiered accreditation

Section 4.7.1 of the Framework states that the ACCC is considering how tiered accreditation should be facilitated across the CDR system. As part of this, the ACCC is seeking views on whether the accreditation system should be CDR-wide or sector-specific. A key matter for consideration appears to be what data sets should be able to be received by persons at particular 'tiers' of accreditation, with such decisions being informed by the sensitivity level of the data sets in question. For example, the ACCC is considering whether it would be appropriate to create lower tiers of accreditation that would allow persons to receive less sensitive CDR data across CDR sectors (subject to appropriate restrictions) or receive only energy data.

By way of general comment, the OAIC appreciates the underlying policy objective to encourage increased participation in the CDR system. However the OAIC would be concerned if tiered levels of accreditation were to create or increase privacy risks that are unable to be appropriately mitigated. The OAIC therefore recommends that any changes to accreditation requirements be carefully tailored to mitigate the risks posed by the specific data handling activities of the relevant entities, and in a way that ensures the privacy and security risks are managed consistently across the scheme and the overall integrity of the CDR system is maintained.

In particular, the OAIC recommends that accredited persons at all tier levels should remain subject to the Privacy Act (see s 6E(1D)), as well as the strong consent, notification and other transparency requirements that currently apply to accredited persons in the CDR, for example in Division 4.3 of the existing Rules. This will help to retain consumer trust in the CDR system.

Section 4.7.1.4 also notes that the ACCC is considering how to ensure the costs associated with accreditation at other tier levels are lower than for the current 'unrestricted' level. The OAIC strongly supports the ACCC's intention to ensure that lower costs do not impinge on the ability of an entity to handle data securely.

Recommendation 6

The OAIC recommends that any changes to accreditation requirements should be carefully tailored to mitigate the risks posed by the specific data handling activities of the relevant entities, and in a way that ensures the privacy and security risks are managed consistently across the scheme and the overall integrity of the CDR system is maintained.

In particular, the OAIC recommends that accredited persons at all tier levels should remain subject to the Privacy Act (see s 6E(1D)), as well as the strong consent, notification and other transparency requirements that currently apply to accredited persons in the CDR.

Lower tiers of accreditation for 'less sensitive' CDR data

CDR-wide

The OAIC understands from section 4.7.1.3 that the ACCC is considering the creation of a lower tier of accreditation that would allow persons to receive 'less sensitive' CDR data across CDR sectors, subject to appropriate restrictions.

While we would consider any further evidence that comes to light as a result of the consultation process, the OAIC has initial concerns about creating a lower tier of accreditation that would allow parties to receive certain classes of ('less sensitive') CDR data across sectors. As outlined in the introduction of this submission, as CDR is rolled out across the economy and data sets can be combined, richer and more granular insights may be derived about individual consumers, meaning the overall privacy risks for consumers may increase.

Sector-specific

As per section 4.7.1.2 of the Framework, if feedback is received in support of the position that energy data is less sensitive than banking data, the ACCC will consider whether it is appropriate to create a lower tier of accreditation to access energy data.

As noted in the introduction to this submission, the OAIC would be concerned if privacy protections under the Rules were to be diluted on the basis of an assumption that energy data is considered to be less sensitive than banking data.

Should the ACCC explore the possibility of having a lower tier of accreditation for energy data further, the OAIC would recommend the ACCC identify and analyse the specific privacy risks posed to consumers by the handling of their energy data.

In particular, as part of this, the OAIC would seek to work with the ACCC on the criteria used by the ACCC to determine the 'sensitivity' level of a given data set. In our view, 'sensitivity' is multi-faceted and complex, and a number of factors may be relevant, for example:

- What insights can be gained about individual consumers from the data? How granular and/or invasive are those insights?
- What are the potential use cases for these types of energy data? What level of risk might those use cases pose for consumers?
- What is the level of comfort in the community in relation to use of this data? What would a well-informed consumer expect in relation to the handling of such data?
- What could the consequences be for a consumer should their energy data be subject to unauthorised access, for example in a hacking incident? How attractive is the data to malicious third parties?

The OAIC therefore recommends that the ACCC gather and consider evidence about the potential privacy risks for consumers from the handling of their energy data as part of their exploration as to whether a lower tier of accreditation to access energy data is appropriate.

Recommendation 7

The OAIC recommends that the ACCC gather and consider evidence about the potential privacy risks for consumers from the handling of their energy data, as part of their exploration of whether a lower tier of accreditation to access energy data is appropriate. The OAIC further recommends this exercise occur ahead of CDR being launched in the energy sector.

Mitigating privacy risks posed by tiered accreditation

The OAIC's understanding from section 4.7.1 of the Framework is that one way in which the ACCC is proposing to mitigate privacy risks is to limit what data sets can be received by persons accredited at a lower level.

As outlined above, the OAIC would be concerned if tiered levels of accreditation were to create or increase privacy risks that are unable to be appropriately mitigated. The OAIC therefore recommends the ACCC consider a broad range of strategies for mitigating privacy risks posed by tiered accreditation. By way of example, it may be appropriate to limit the format in which a person accredited at a lower level may receive CDR data (i.e. to a modified, lower-risk format), or provide that the person can only use CDR data for specific purposes that have been subject to careful consideration, and deemed to be lower-risk.

The OAIC notes that any such mitigation strategies will need to be tailored to the specific risks posed by the specific data handling activities of the relevant entities, which may not yet be known.

Recommendation 8

The OAIC recommends that the ACCC consider a broad range of strategies for mitigating privacy risks posed by tiered accreditation. By way of example, it may be appropriate to limit the format in which a person accredited at a lower level may receive CDR data (i.e. to a modified, lower-risk format), or provide that the person can only use CDR data for specific purposes that have been subject to careful consideration, and deemed to be lower-risk.

Interaction between the Rules and data standards

General approach

The OAIC understands from section 3.3 of the Framework that the ACCC's general approach to making Rules on data sets is to specify minimum inclusions of key data (i.e. to add further detail to the broad categories set out in the energy sector designation instrument), while allowing flexibility for additional refinement and specification of data sets in the standards. We further understand that this is consistent with the approach taken in the banking-specific Rules. The OAIC is broadly supportive of this general approach.

The OAIC further understands, from section 4.1.1.1 of the Framework, that the ACCC will continue to work closely with the Data Standards Body, Data61, as they assist the Data Standards Chair to make energy data standards. The OAIC supports this, noting the importance of ensuring that the Rules provide an appropriate level of detail to inform the development of relevant data standards.

On a related note, the Framework outlines in section 3.3.5 how the ACCC is proposing to make a Rule that adopts the definition of 'distributed energy resources' register data in the energy sector designation instrument, while providing flexibility for the data standards to determine which aspects of this register data will be in scope for sharing. The OAIC notes that this proposal does not appear to align with the ACCC's general approach of specifying the minimum inclusions of key data in the Rules, and would suggest the ACCC consider providing greater specificity here, where appropriate and practicable.

Customer data

The OAIC understands, from section 3.3.2 of the Framework, that the ACCC is seeking views on whether any particular types of information should be excluded from customer data on the basis of sensitivity, or if not excluded, presented separately in the consent process from other data sets (and as a discrete data cluster) to enable greater consumer control over sharing and use of this data. Examples of such data might include hardship information, and concession details.

The OAIC notes that the broad categories of customer data have been designated as CDR data in the designation instrument, and that there appear to be valid use-cases for all these types of information. In light of this, and from an information access perspective, the OAIC's preference would be for particularly sensitive subsets of customer data to be set out in the data standards as a discrete data cluster (i.e. 'type' of CDR data)[21]rather than excluding the data. This will increase the granularity of consumer control in the sharing of their data.

Dashboards

The Framework considers in section 4.4 that a different approach to data holder consumer dashboards is warranted for the energy sector. This is because data sets comprising a consumer's electricity supply will be held by more than one type of data holder (e.g. retailers and AEMO). Under the existing Rules, a consumer would be provided with multiple data holder dashboards and would need to visit each of these to withdraw an authorisation to share a data set for a single product.

In section 4.4, the Framework outlines that the ACCC's preference for the energy sector is for one party to be responsible for providing the data holder dashboard, in relation to 'all consumer data requests for a consumer'. The OAIC assumes that this refers only to energy-related consumer data requests, not all consumer data requests made under the CDR. Based on this understanding, the OAIC supports this proposal as it is privacy-enhancing and will ensure a simpler consumer experience (a consumer will only need to engage with one dashboard to manage their authorisations). The OAIC also supports the intention to keep the approach to accredited person consumer dashboards in energy consistent with that set out in the existing Rules.

By way of general comment, the OAIC considers that any process set out in the Rules for providing the data holder consumer dashboard must be supported by robust privacy and security settings, including appropriate data handling limitations on the dashboard provider and any third party service providers engaged by the dashboard provider. For example, the dashboard provider should only use any additional information collected for dashboard-related purposes. We appreciate that the specific privacy protections that are necessary may only become apparent as the technical options for the dashboard develop.

The Framework presents three options for a single, consolidated data holder dashboard: (1) the consumer's current retailer provides the dashboard; (2) AEMO provides the dashboard; or (3) the consumer's current retailer provides the dashboard through an AEMO-provided interface.

The Framework clarifies that to be able to provide a dashboard to a consumer, the dashboard provider would need to have some way of authenticating the consumer. For Option 1, the consumer's current retailer will already hold the relevant consumer data needed for

[21] When asking a consumer to consent to the collection and use of their CDR data, an accredited person must allow the consumer to actively choose particular 'types of CDR data' to which they are consenting to the accredited person collecting (Rule 4.11(1)(a)). A 'type' of CDR data means a type of data that is identified in the data standards (Division 1.3).

authentication. However, for Options 2 and 3, AEMO would need to access or hold this consumer data (which they currently do not hold) in order to authenticate the consumer and provide the dashboard.

The OAIC therefore recommends the ACCC adopt 'Option 1' for the provision of data holder consumer dashboards in the energy sector. Option 1 builds on the existing consumer-retailer relationship, which will be most seamless and logical from a consumer experience point of view, and would appear most consistent with the approach taken in the banking sector. Further, under Option 1 the retailer already holds the relevant consumer data needed for authentication and would not need to expand its personal information holdings to provide the dashboard.

Finally, the OAIC notes that Options 1 to 3 would likely require Rules to be made to require retailers or AEMO (as relevant) to notify the dashboard provider of the disclosure of CDR data. This is because energy data will likely be held by multiple data holders, and this information will need to be reflected in the single, consolidated data holder dashboard. If such Rules are made, the OAIC would suggest clarifying through the Rules that only data necessary for the provision dashboard services should be included in the notification.

Recommendation 9

The OAIC recommends that the ACCC adopt 'Option 1' for the provision of data holder consumer dashboards in the energy sector. More generally, the OAIC considers that any process set out in the Rules for providing the data holder consumer dashboard must be supported by robust privacy and security settings, including appropriate data handling limitations on the dashboard provider and any third party service providers engaged by the dashboard provider.

Approach to 'eligible' CDR consumers in the energy sector

Section 4.2 of the Framework considers which CDR consumers should be considered 'eligible' CDR consumers for the purposes of the energy sector. The ACCC's ability to define an 'eligible' CDR consumer in the Rules is limited by the definition of 'CDR consumer' in section 56AI of the Consumer and Competition Act, which in part requires that CDR data relates to the person because of the supply of a good or service to the person, or to one or more of their associates (e.g. their spouse or relative), and that the person is identifiable or reasonably identifiable from the CDR data. While 'CDR consumer' is defined in the Competition and Consumer Act, only 'eligible' CDR consumers can make consumer data requests for the transfer of their CDR data under the Rules.

The Framework considers whether joint account holders and nominated persons should be eligible consumers and proposes to restrict eligibility to individuals over 18 years of age. It also considers the possibility of allowing consumers with inactive and offline accounts into the CDR system. As noted in section 4.2.1 of the Framework, where the ACCC considers there are persons who should be eligible consumers but do not meet the legislative definition of 'CDR consumer', regulations would need to be made to bring them within the scope of the CDR for energy.

Protections for identifiable persons living in the premises, who are not CDR consumers

The Framework outlines the ACCC's general approach to eligible consumers in section 4.2.3.1, which is to require a CDR consumer to have an account with a retailer to be considered an eligible CDR consumer. Linking eligibility to an account holder ensures that only persons who are 'known'

to the retailer can consent to the sharing of their CDR data. However as noted in section 4.2.3.1 of the Framework, a consequence of this approach is that CDR data may be shared irrespective of whether the requesting consumer resides at the premises to which the CDR data relates. By way of example, this would mean a landlord (as the account holder) could request and share energy CDR data in relation to the premises which they do not themselves occupy.

This raises privacy risks, including that a landlord would have access to energy data from which they may be able to infer certain behaviours and derive other granular insights about the tenants (that the tenant/s may not be comfortable with). The ACCC is therefore seeking feedback on whether and how Rule 4.12(3)(b) should be tailored to the energy sector to address these risks. Rule 4.12(3)(b) prohibits ADRs from using CDR data to profile individuals who are not the consumer who made the request.

The OAIC agrees with the privacy concerns outlined above and supports the exploration of additional Rules that may be required to ensure ADRs do not profile identifiable individuals who live at the premises but are not the CDR consumer. This is important given our understanding that energy data can reveal granular insights about all occupants in a property, and that it is likely transfers of energy CDR data may be effected by those who do not live in the property.

By way of example, the Framework proposes making a Rule to prohibit the sharing of information that would identify persons living in the premises who are not the CDR consumer that made the data sharing request. The OAIC supports this proposal.

Including nominated persons as 'eligible consumers'

The ACCC is seeking views on which nominated persons may be eligible CDR consumers. The ACCC clarifies in section 4.2.3.1 that for the purposes of the Framework, a nominated person is a person who has been authorised to transact on the account by the account holder (known as 'customer authorised representatives' under national energy legislation). Examples of nominated persons include financial counsellors and family members who may or may not occupy the premises.

The ACCC acknowledges however that retailers may have varying levels of nominated persons (i.e. depending on the specific arrangement, a nominated person may have differing levels of access and scope to make changes to the account). The ACCC is therefore seeking to understand from retailers how nominated person arrangements are characterised in practice.

The Framework notes in section 4.2.3.1 that not all nominated persons would meet the existing definition of 'CDR consumer' in section 56AI of the Competition and Consumer Act. This is because a CDR consumer must be supplied the service (or be an associate of the individual to whom the service is being supplied).

At this stage, the OAIC would caution against expanding the scope of 'eligible CDR consumer' for the energy sector to include nominated persons that would not already be captured as CDR consumers under the Competition and Consumer Act. As an eligible CDR consumer, any nominated person, regardless of the particularities of their nominated person arrangement, would be able to make consumer data requests for the transfer of energy data. This may not be appropriate where a nominated person has limited authority over and access to the energy account.

By way of general comment, in considering whether certain nominated persons should be eligible to make consumer data requests, the OAIC suggests regard should be given to the existing terms of the nominated person arrangement and commensurate permissions be applied in terms of their participation within the CDR system. We suggest this be considered further in light of evidence gathered by the ACCC from retailers about how nominated person arrangements work in practice –

such evidence may reveal a compelling policy reason for including certain classes of nominated persons as eligible consumers.

Approach to authorisation for joint account holders

The ACCC is proposing to make Rules to the effect that where consumers with a joint account hold individual authority to transact on the account (i.e. do not require the other account holder's consent to transact), they will be within scope as eligible CDR consumers (section 4.2.3.1 of the Framework).

The ACCC clarifies in section 4.2.3.1 that for the purposes of the Framework, a 'joint account holder' is an individual who is considered a primary account holder, has full permissions to act on the account and is financially responsible for the account. However, the ACCC is seeking stakeholder views on whether this characterisation of a 'joint account holder' is accurate.

The Framework suggests that a Rule requiring a joint account management service is not necessary for the energy sector. This because the ACCC considers that where there already exists an individual authority to transact on the account, this will be a sufficient basis upon which a consumer can share data related to that account. This contrasts with the approach taken in the banking sector, in which each joint account holder must elect through a joint account management service for a joint account to be 'in scope' for CDR data sharing.

The OAIC suggests the utility of a joint account management service may need to be considered further in light of evidence gathered by the ACCC about how joint account holders work in practice in the energy sector. For example, if during consultation it becomes apparent that joint account holders do not always have individual authority to transact on the account, it may be appropriate to require some form of a joint account management service.

The OAIC understands from section 4.2.3.1 of the Framework that Data61's consumer experience research findings influenced the decision to require a joint account management service in the banking sector (Data61's research found that multi-party authorisation was the preferred method of accessing banking joint accounts by most research participants). The OAIC therefore suggests that the ACCC work with Data61 to ensure consumer experience research is undertaken to confirm whether consumers would be comfortable with not having multi-party authorisation for the sharing of CDR data in the energy sector.

Offline and online accounts

The Framework sets out at section 4.2.3.4 that there is a large percentage of consumers who either do not have an online account, or do not use their online account as the dominant mode of communicating with their retailer. The Framework therefore proposes not to limit those who lack an online account (i.e. have an 'offline account') from being eligible consumers.

The OAIC's understanding is that consumers would be able to exercise their rights under CDR using offline mediums such as telephones (for example: to provide and withdraw consent and authorisation; elect for their redundant CDR data to be deleted; and receive CDR receipts and other ongoing notifications required to be given under the existing Rules). However, we have assumed that the transfer of CDR data would continue to occur in the usual 'online' manner through the data standards, according to the same stringent security arrangements currently in place.

Based on this understanding, and from an information access perspective, the OAIC is supportive of extending the definition of eligible consumer to also include consumers with offline accounts.

The Framework acknowledges that, should consumers with offline accounts be included, the ACCC will need to consider the impact on existing obligations for data holders and ADRs to provide a consumer dashboard. This is because the Rules currently require these dashboards to be provided as an 'online service'.[22]

The OAIC agrees with this, and considers that there are several matters to be worked through in the existing Rules to ensure 'offline' consumers have access to the full suite of transparency measures that online consumers have under the existing Rules. For example, new Rules would be required under Privacy Safeguards 5 and 10 to allow ADRs and data holders to notify of the collection/disclosure of CDR data in an offline manner otherwise than through the consumer dashboard.[23]

Further, the OAIC would recommend making appropriate changes to the information security controls in Schedule 2 of the existing Rules to account for offline mediums, and to ensure that privacy protections are not diluted as the mediums through which consumers can engage with the CDR system expand.

In light of the above, the OAIC suggests that the ACCC consider further how including consumers with offline accounts will impact on obligations on data holders and ADRs in the existing Rules, and how it should affect the development of relevant Rules for the designated gateway.

Recommendation 10

The OAIC recommends the ACCC consider further how including consumers with offline accounts will impact on obligations of data holders and ADRs in the existing Rules, and how that arrangement should affect the development of relevant Rules for the designated gateway. Adjustments or additional requirements may need to be made to the Rules in light of this review. For example, the OAIC would recommend that appropriate changes be made to the information security controls in Schedule 2 of the existing Rules to enable offline participation, and to ensure that privacy protections are not diluted for those using offline mediums to engage with the CDR system.

Inactive accounts

For the initial scope of CDR in energy, the ACCC is considering limiting eligible consumers to those that have an active account with an electricity retailer (i.e. are currently in a retail contract for the supply of electricity). The Framework at section 4.2.3.3 seeks stakeholder views on whether there are compelling use cases for the sharing of retailer held data sets for 'inactive accounts', to inform considerations of whether inactive accounts should be brought in scope at a later time. An inactive account refers to an account previously held by a consumer before they switched retailer providers. The OAIC is broadly supportive from an information access perspective to extend the definition of eligible consumer to include energy consumers who have an inactive account with a retailer. We note this means that consumers will be able to securely transfer their data in relation to an inactive account to an ADR.

[22] CDR Rules 1.14 and 1.15.

[23] Rule 7.4 (in relation to Privacy Safeguard 5) and Rule 7.9 (in relation to Privacy Safeguard 10) require an ADR and data holder to notify the consumer of several matters in relation to the collection/disclosure of their CDR data through the consumer dashboard.

The Framework outlines, in section 4.2.3.3, certain additional requirements that may need to be imposed on data holders if the definition of eligible consumer is extended to those who have inactive accounts. These relate to authorisation and additional steps in the authentication process. The OAIC supports these additional requirements, and generally notes the importance of strong authentication models and processes to securely verify a consumer's identity, as outlined further below.

Minors

At section 4.2.3.2 the Framework suggests that consumers under the age of 18 should initially be excluded from being considered eligible consumers. The OAIC supports this recommendation as it is consistent with the approach taken in the banking sector. It also recognises that minors comprise only a small proportion of account holders with electricity retailers.

Authentication

The Framework notes in section 4.3.1 that in considering consumer authentication, there is a balance to be struck between ensuring security of data sharing and a satisfactory consumer experience. As the ACCC considers how the Rules should provide for authentication of consumers in the energy sector, the ACCC's view is that the balance should be weighted towards ensuring a high degree of security for consumer data, whilst minimising consumer friction. The ACCC further notes that they consider it appropriate to follow a similar approach to authentication as is currently used for the banking sector (i.e. the 'redirect model', which is a type of 'strong authentication'). By way of overall comment, the OAIC supports this general approach to consumer authentication in the energy sector.

The Framework proposes two authentication models in section 4.3.4. In Model 1, the consumer's current retailer (with whom the consumer has a pre-existing relationship) would be responsible for authentication. This would leverage the retailer's existing authentication processes (some of which may be offline). In Model 2, AEMO (with whom most consumers will not have a pre-existing relationship) would be responsible for authentication, using consumer contact details provided by the consumer's retailer. The Framework notes in section 4.3.4.3 that the ACCC's preferred model is Model 1.

The OAIC supports the ACCC's preference for Model 1 and recommends that the ACCC adopt Model 1 for authentication of consumers in the energy sector. We understand Model 1 has less complex information flows and is consistent with the approach taken in the banking sector. We further understand that Model 1 would include offline authentication processes where already used by the retailer. In this regard, the OAIC would recommend the ACCC ensure the same high level of security that exists for online authentication can be achieved by offline authentication processes.

The OAIC notes Model 2 would require a consumer's personal information to be transferred from data holders to AEMO for the purpose of authentication and would caution against taking an approach which unnecessarily increases AEMO's personal information holdings. This is consistent with the OAIC's preference for the AEMO gateway to function as a 'conduit' in the CDR system.

The Framework notes in section 4.3.3.1 that there are several energy-specific factors that may warrant a departure from the approach to authentication used in the banking sector. One of these factors is the likelihood that ADRs will need data from more than one data holder for certain use cases. Given that an energy consumer is likely to have a single electricity supply service, the ACCC proposes that customers should only have to authenticate with one data holder (i.e. their current retailer). It appears from the Framework that this departure from the banking approach is

warranted because banking consumers are likely to have multiple financial products with multiple data holders.

While the OAIC understands that authentication through a single data holder would be more convenient for the consumer, we consider that to ensure transparency, the consumer should be made aware of the terms of the authentication arrangement (i.e. that other data holders would be relying on the single authentication from the consumer). The OAIC would therefore suggest the ACCC consider making an energy-specific Rule that requires such a notification to be given.

The Framework also seeks stakeholder views at 4.3.3.1 on whether it would be appropriate to adopt an alternative or additional method of authentication for certain AEMO-held data sets. This would involve sharing of data sets on the basis of the consumer being able to provide the national metering identifier, postcode and name of the current retailer for the relevant premises (in contrast to 'strong authentication' which relies on the consumer's identity).

By way of general comment, the OAIC would caution against the use of 'weaker' authentication models as these may dilute the high degree of security currently needed for consumer authentication in the CDR system. However, we would be interested to consider the evidence gathered during consultation (for example whether there are specific, lower-risk use cases in which weak authentication might be appropriate).

Recommendation 11

The OAIC supports the ACCC's preference for authentication Model 1 and recommends that the ACCC adopt this model for consumers in the energy sector. Given that Model 1 may encompass offline authentication processes, the OAIC further recommends the ACCC ensure the same high level of security that exists for online authentication can be achieved by offline authentication processes.

Implementation matters

Dispute resolution

The OAIC is supportive of the Framework's proposed approach at section 4.5 for the internal dispute resolution (IDR) Rules for the energy sector to align with the existing requirements set out in the National Energy Retail Law and the Energy Retail Code (Victoria). We consider taking this sector-specific approach will ultimately be easier and more efficient for the consumer. For example, in the event a consumer's complaint raises both CDR and non-CDR issues, having the IDR process aligned with the CDR participant's existing requirements could mean the complaint could be considered holistically, rather than having elements of a complaint separated and dealt with by different entities. Further, this would mean the consumer would not have to participate in separate dispute resolution process. Rather, they can engage in processes they may already be familiar with, as part of their existing relationship with their retailer.

We understand there may be future consideration of whether the Rules for IDR processes should include complaints made by CDR entities, however this is not being addressed in the development of the Rules. Expanding IDR processes to include complaints by CDR entities may go beyond the intention of the CDR scheme, which is focused on the rights of consumers and businesses over how their data is shared. Further, CDR participants are more likely to have the resources to seek legal advice or commence legal proceedings than consumers are.

Phased implementation

The OAIC is supportive of the adoption of a phased implementation approach (similar to banking), to be achieved by bringing the largest energy retailers into the regime first and then phasing remaining retailers in a second tranche. We note that the ACCC has initially proposed using a retailer's customer numbers as the threshold determining which tranche of implementation they will be involved in and is seeking stakeholder views on whether this is appropriate.

The Framework also proposes to exclude certain small retailers from data sharing obligations if they fall below a certain threshold (section 4.6). From an information access perspective, the OAIC queries why this exclusion is being proposed, as it would prevent certain consumers from accessing or transferring their data through the CDR based on their retailer. We note that no such exclusions apply in the banking sector, where there are also many 'small players' (such as newly established 'neo-banks' that still have data sharing obligations). In the absence of a compelling policy reason, the OAIC suggests the ACCC consider whether appropriate risk mitigation strategies could be put in place as an alternative to excluding smaller energy retailers as data holders under the CDR.