Wil

ESB Data Strategy

Preliminary legal report

Prepared by KWM and Galexia for the Energy Security Board

31 July 2020

Asia Pacific | Europe | North America | Middle East

KWM.COM

Contents

Terms of use

The material in this report is provided as information only and does not constitute legal or other advice on any specific matter. Users of this report requiring or seeking legal advice are responsible for obtaining such advice from their own lawyers, and should do so before taking, or refraining from taking, any action in reliance on any information on this report. This report is not intended to and does not create any client/lawyer relationship between any user and any King & Wood Mallesons network firm.

The term “user” above means the individual accessing this report and where that access is made in a business context, any company or other organisation of which that individual is an officer, partner, member, employee or agent and other members of the same group as that company or other organisation to whom information in this report is passed.

A. Executive Summary

This report identifies that public bodies face three broad challenges to greater sharing of energy data between themselves and with other public interest bodies. These are:

- **complexity of legislative regime** – the law starts with a prohibition on data sharing, followed by various, sometimes inconsistent exceptions. This complex legal landscape, developed in a past-era, leaves data holders uncertain about how to interpret the law and how to safely share energy data with other public bodies;
- **unworkable public interest test** – the current framework contains a public interest data sharing regime, however, the public interest test within it is vague and the regime itself is difficult to implement; and
- **privacy concerns and commercial sensitivities** – these have been the driving concerns, limiting the sharing of energy data under the existing regime.

This report identifies a series of potential, high-level reform options for consideration, to address these challenges. The options range from the creation of consistent data policies at the level of guidelines and procedures, to a complete overhaul of the existing regime at the law level.

A Glossary of acronyms is included in **Appendix 1**.

1 Context

KWM and Galexia have been asked to provide preliminary legal advice on options for reforming energy laws to support the implementation of the ESB's Data Strategy.

The ESB has been tasked with the design of a Data Strategy to support the transformation of the energy sector for the benefit of all Australians. The ESB's Data Strategy aims to address digitisation and the transition to new technologies in the energy sector. In particular, the Data Strategy focuses on the continuous improvement of data management and support systems in the face of increasing volumes of data and cyber security concerns. The Data Strategy recognises that the data needs of the energy sector have fundamentally changed since the creation of the current regime, which is no longer fit for purpose, and not fit for the future where data will be of increasing importance.

The Data Strategy seeks to guide the AEMC, AER, AEMO and a range of relevant public bodies (such as the ACCC, CER, ABS, DISER and jurisdictional regulators) to identify and manage their data needs and those of the energy sector – including market participants, consumers, service providers and researchers.

Importantly, the ESB Data Strategy aims to bring energy laws into line with current needs and recent shifts in data policy. This preliminary report is provided within the context of significant legislative and policy reform occurring across the energy sector and the Australian data landscape.

Key initiatives considered in the preparation of this advice include:

- National Energy Analytics Research Program;
- ACCC Retail Electricity Price Inquiry;
- "Big stick" legislation;
- ESB Two-Sided Market Report;

- the establishment of the National Data Commissioner;
- the release of the Department of Prime Minister and Cabinet's "Best Practice Guide to Applying Data Sharing Principles";
- the ONDC's Data Sharing Agreement Template for consultation;
- the Consumer Data Right legislation within Part IVD of the CCA (**CDR**); and
- the proposed "Data Availability and Transparency Act" (**DAT Act**).

See **Appendix 2** for a summary of the above initiatives.

2 Scope

The ESB has engaged KWM and Galexia to provide this preliminary report on options for reforming energy laws to better support data management and optimisation amid the ongoing transformation of energy markets into a data-driven future. This preliminary report forms part of a broader workstream being undertaken in the ESB's Data Strategy. Accordingly, this report addresses a more limited scope than the ESB's Data Strategy and will focus on the sharing of publicly held datasets between:

- "**Core Bodies**" (being the AEMC, AER, AEMO and ESB);
- "**Trusted Bodies**" (such as the ABS, ACCC, CER, ARENA and DISER); and
- research bodies and public bodies outside the energy sector (such as CSIRO and universities).

This report is structured as follows.

1 **Understanding the problem –** a summary of issues faced by energy market bodies attempting to share public sector energy data under the current regime. This part provides analysis of the ways the current energy laws and regulations limit effective data collection, use and sharing by the Core Bodies and Trusted Bodies. This part has been prepared by KWM – see Part B.

2 **Approaches to data regulation –** a preliminary review of approaches to facilitating access to data in other sectors within Australia and internationally. A summary of key lessons and emerging best practice is provided. This part has been prepared by Galexia – see Parts C and D.

3 **Reform pathway –** a summary of potential implementation steps to drive reform, including high-level options to improve the existing regime (involving both legislative and non-legislative options) and an "overhaul" option, which involves fundamental reforms to the use and sharing of energy data. This part has been prepared by KWM – see Part E.

The following items were considered out of scope for the purposes of this preliminary report, but are likely to form part of a second phase and more detailed legal report, to be considered after public consultation on the options presented here:

- consideration of jurisdiction-specific laws and state-based energy bodies;
- a detailed review of barriers and inconsistencies in the current regime, on an individual Rule/Regulation level, including consideration of "data gaps" where expanded collection rights may be required; and
- more detailed legal design of the options proposed in Part E.

3 Summary of findings

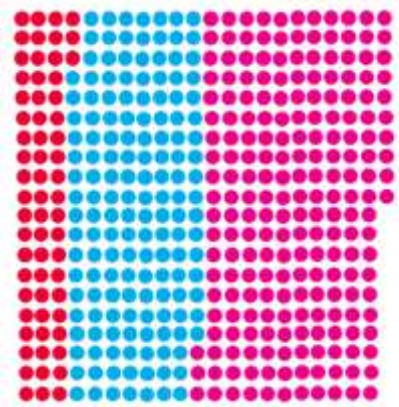
Step 1: Understanding the problem

Reform options proposed in this report must be measured by their ability to overcome the challenges to data sharing within the current legislative environment. The reforms must provide energy market bodies sufficient support and clarity to move the dial from the current state of conservatism around data sharing between energy market bodies, towards frequent, efficient and safe data sharing. As such, an essential first step was to investigate the current issues associated with data-sharing to then identify the root-cause of those issues.

Through a high-level request for information (**RFI**) issued to the Core Bodies and DISER (formerly DEE), we identified several initial issues that these stakeholders currently face in collecting, using and sharing energy data. The following issues are best described as symptoms of a broader problem, arising from the current regulatory framework:

- **duplication of collection** – ACCC, AEMC, AER, ABS, ECA and CSIRO undertaking separate consumer surveys to obtain similar data in relation to retail energy bills and usage. The AEMC also gave the example of overlap between the ACCC and the AER's role in monitoring and reporting on the contract and wholesale electricity markets;
- **use of undesirable workarounds** – for example, Trusted Bodies scraping data from the Energy Made Easy website due to the AER's inability to share tariff data in a more useful form, despite it being published;
- **lengthy and costly bilateral sharing arrangements** – spending significant cost and resources on complex and lengthy contractual negotiations to allow AEMO to share data with CSIRO under the National Energy Analytics Research program (**NEAR**), where sharing remains constrained;
- **stalled or abandoned sharing negotiations** – spending effort and resources on attempts to create workable sharing arrangements when ultimately, no data was able to be shared. The AEMC gave the example of attempting to access ACCC data under section 157A of the CCA; and
- **data gaps** – useful data not currently being collected by any of the Core Bodies or Trusted Bodies. Usually, this is because the data was not previously available or needed, however, with new technologies and increased competition in an ever-more complex market, this data may now be needed for effective planning and operation. Capturing this data would require new areas of policy development and supporting legislation. In some cases, filling these data gaps would require legislation to cover entities not currently regulated by the energy regime (such as EV charging station installers). Although we have provided a list of the data gaps identified by the Core Bodies during the limited RFI process in **Appendix 3**, changing data needs in the future will mean that new data gaps will continue to emerge. An analysis of data gaps is not within the scope of this report.

After identifying these issues, we developed a hypothesis that the current legislative regime restricts the sharing of energy data and lacks the flexibility required to adjust to changing data needs over time. To test this hypothesis, we undertook a detailed mapping of data collection, use and sharing provisions in the current legislative regime. We mapped and analysed:



125 relevant provisions in the NGR

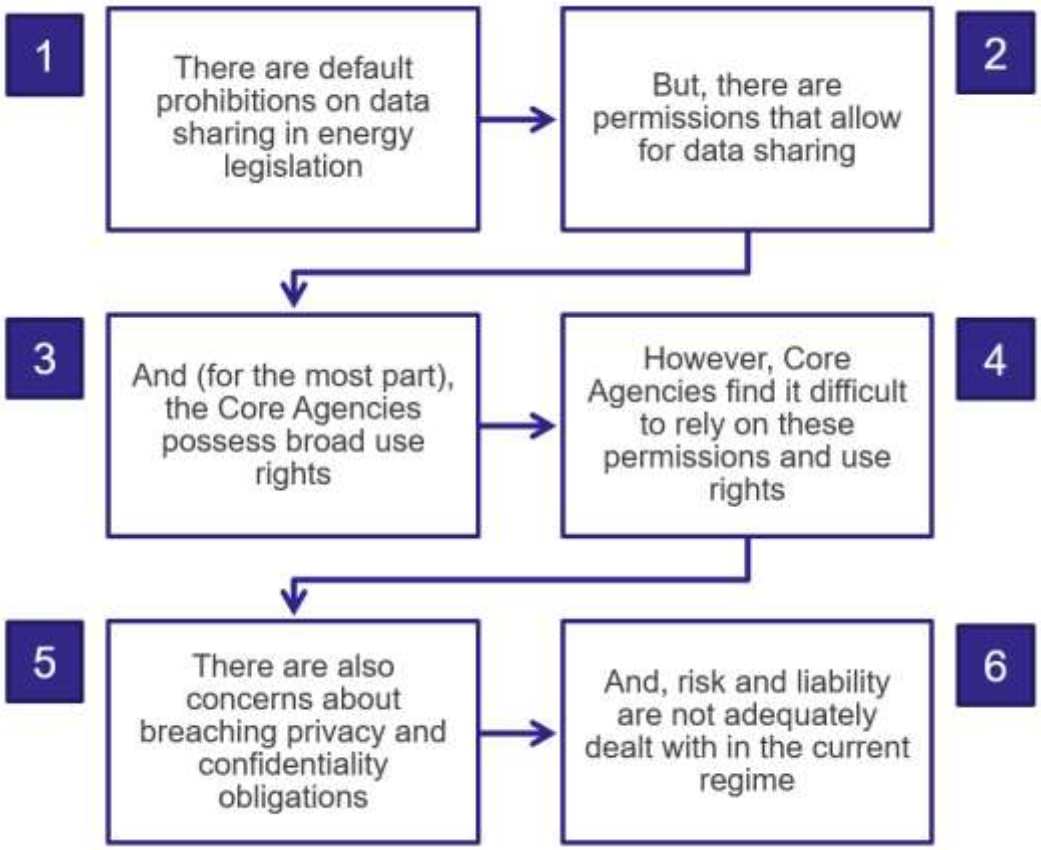
308 relevant provisions in the NER and NERR

427 relevant provisions across 10 different laws and regulations relating to gas and electricity

Ultimately, this mapping exercise revealed that:

- a very large number of collection, use and sharing provisions of varying levels of prescription exist across legislation, rules, regulations and procedures;
- there was no clear, overarching approach to those provisions or their level of prescription;
- there was a lack of clarity in the interaction between these provisions and other relevant regimes, eg privacy; and
- in some cases, there were inconsistencies within and across legal instruments.

From this mapping exercise, we identified the following underlying causes of the symptoms experienced by the Core Bodies:



Our analysis led us to the view that energy market bodies face three broad, conceptual challenges. These are:

- **complexity of legislative regime** – the law starts with a prohibition on public sector data sharing, followed by various, sometimes inconsistent exceptions. This complex legal landscape, developed in a past-era, leaves data holders uncertain about how to interpret the law and how to share energy data safely with other energy market bodies;
- **unworkable public interest test** – the current framework contains a public interest data sharing regime, however, the public interest test is vague and the regime itself is difficult to implement; and
- **privacy concerns and commercial sensitivities** – which have been the driving concerns, limiting the sharing of energy data under the existing regime.

Step 2: Approaches to data regulation

Our second step was to analyse local and international approaches to data regulation for insights for the ESB's Data Strategy in Australia. This analysis, led by Galexia, is detailed in Parts C and D below.

This analysis looks at several local data sharing initiatives that may provide useful lessons for the energy sector, including examples from the health and telecommunications sectors. It then compares those examples with more comprehensive data sharing frameworks proposed under the CDR regime and the proposed DAT Act. The analysis of local initiatives identified emerging best practice models for regulating data sharing. It also identified opportunities to leverage data sharing infrastructure (such

as template data sharing agreements and accreditation models) being developed in the broader marketplace for use in the energy sector.

Parts C and D also cover international data sharing initiatives with a direct impact on the energy sector. The examples provide a wide spectrum – from light touch approaches implemented in Singapore and the United States, to more robust approaches implemented (and proposed) in the Netherlands and the United Kingdom. Some of these international examples are particularly focussed on energy data, and many of the initiatives have been implemented (with varying degrees of success).

Overall, the local and international case studies provide valuable insights into best practice measures, including the emergence of the Five Safes model for data sharing, and the switch from restricting the release of data to imposing conditions on the use of data.

Step 3: Reform pathway

Steps 1 and 2 led us to propose three high level reform options for consideration:

- **non-legislative improvements –** a reform package that uses non-legislative mechanisms to address some of the key issues with data collection and sharing;
- **legislative Improvements –** a legislative reform package that addresses some of the identified regulatory barriers, without departing from the overall structure of the current regime; and
- **overhaul –** fundamental, principled changes to the existing confidential information and public interest data sharing regimes to create a new, fit for purpose public benefit data sharing regime.

We also considered the implications of maintaining the status-quo – that is, how the current framework would fare into the future if no changes were made.

It follows that to achieve greater data sharing in the energy sector, the choice of reform options proposed must:

- **build clarity into the legislative regime –** with clarity of policy intention; and
- **drive sustainable change while protecting privacy appropriately –** by gradually fostering a culture that shifts the thinking from "*what are the risks of disclosing data?*" to "*how can this data be safely shared to realise the public benefit*?"

The reform pathway presented in this report has been designed as a dynamic set of options. Each option or step can be actioned if and when the ESB sees fit and will independently create benefits for data sharing.

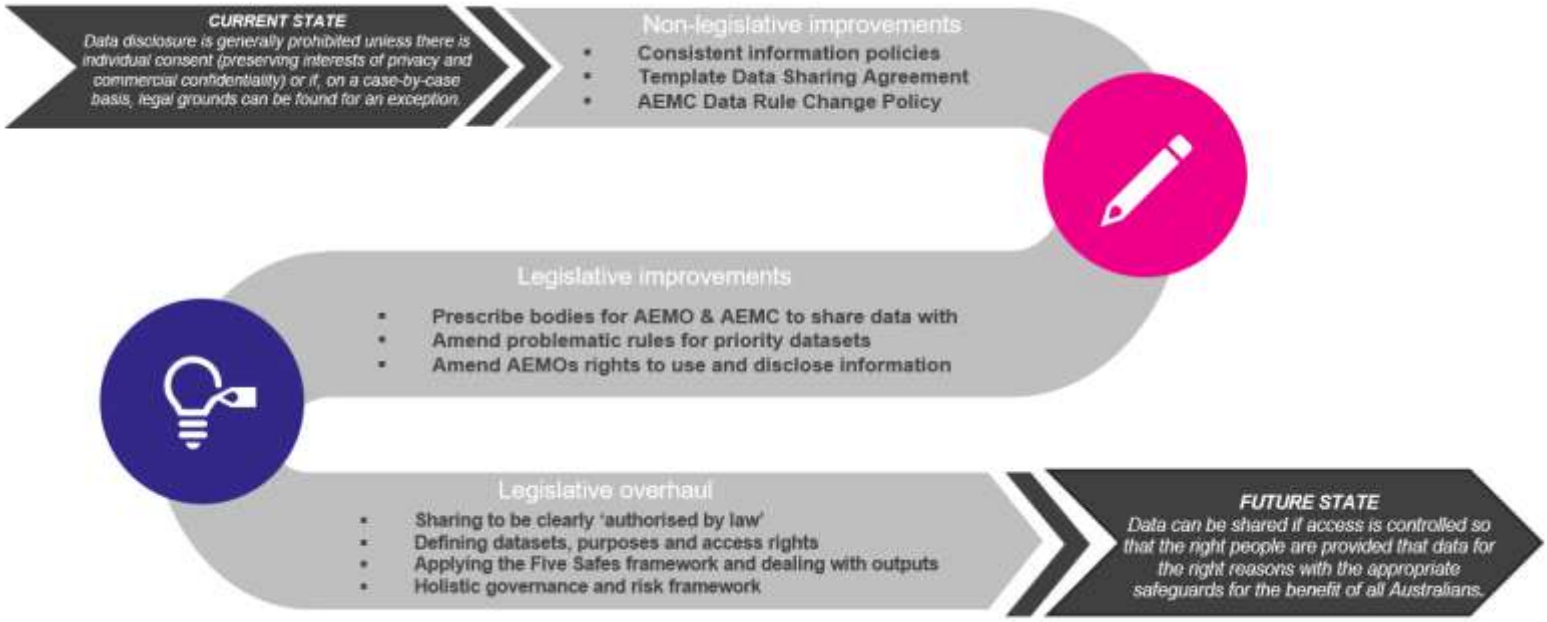
The development of these reform options is likely to be influenced by the timing of two critical data reforms currently underway at the federal level, the CDR and the DAT Act. The sequencing of these reforms currently appears to be:

- **CDR** – the Treasurer has commenced the process for the extension of the CDR to the energy sector. The designation instrument for CDR in energy came into effect on 30 June 2020. The ACCC is actively considering how CDR will be implemented in the energy sector and has released a position paper on the data access model for energy data and on the data access model for energy data. It is now undertaking a consultation into the application of the foundational CDR rules (established for the banking sector) to the energy sector; and
- **DAT Act** – ONDC announced on 22 April 2020 that while they had hoped to consult on an Exposure Draft of the Data Availability and Transparency Bill in the first half of 2020, this has not

been possible with the shift in the Government's priorities in response to the impact of COVID-19. ONDC has not yet publicly released a revised timeframe for consultation.

If the ESB decided that it was prudent to wait for greater clarity around the form and enactment of the DAT Act or the CDR, for example, the non-legislative options presented in this report could be actioned before progressing to more fulsome reform options in the future.

The diagram below sets out a potential pathway from the current state of energy data sharing to the ESB's desired future state, with steps for incremental improvements and more significant reform along the way. This approach could have the benefit of unlocking greater data sharing immediately, while initiating cultural change and building confidence around certain concepts before more significant reform is undertaken. Of course, this pathway need not be followed in a linear fashion – some reforms will take longer to implement than others and completion of them should not delay the commencement of other reform options.



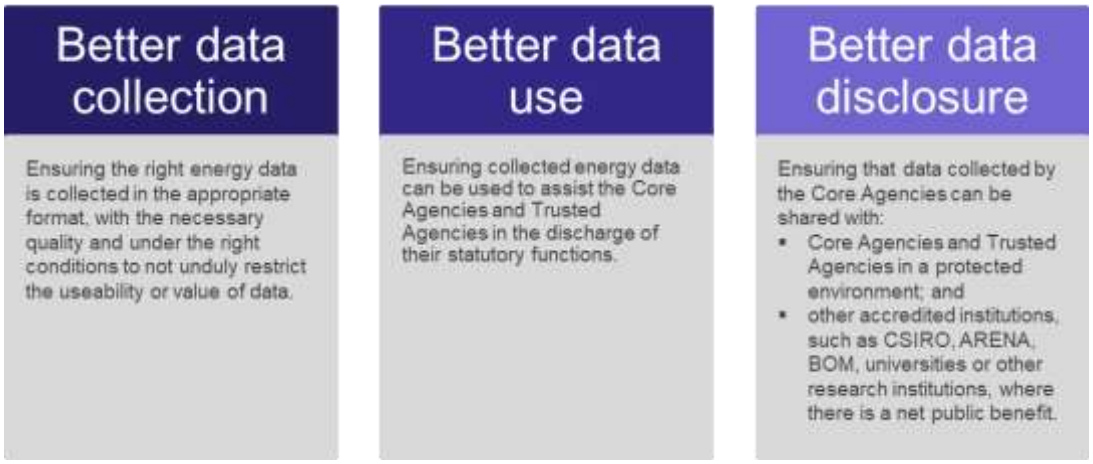
B. Understanding the problem

1 Overview

In this Part B, we have analysed the problem in two parts:

- first, understanding issues with the way energy laws currently protect or permit the use and sharing of data; and
- second, understanding other barriers or restrictions to sharing data arising out of privacy, confidentiality or liability concerns.

The 3 key outcomes below shaped our understanding of the problem and our proposed reform options:



This report adopts the terminology of the Department of Prime Minister and Cabinet's *Best Practice Guide to Applying Data Sharing Principles* where appropriate. Accordingly:

- **data release**: is used to refer to making data publicly available, with no or few restrictions on who may access the data and what they may do with it;
- **data sharing**: is used to refer to making data available to a Core Body, Trusted Body, organisation or person under agreed conditions; and
- **data disclosure**: is used to refer to data release or data sharing under certain legislation, including the NEL, NGL, NERL, relevant Rules, CCA and Privacy Act, where that term is used.

2 Default prohibition on data sharing

The starting point with respect to data subject to energy laws is that all information collected by Core Bodies is protected and should not be shared. We think that this presumption against sharing reflects an underlying belief that energy-related data:

- is inherently valuable to the data provider;
- must be protected because of individuals' privacy and confidentiality concerns; and
- is held by Core Bodies as custodians, requiring those Core Bodies to respect the rights, interests, obligations and expectations that attach to that data.

Set out below is a high-level summary of the general prohibitions against sharing applicable to Core Bodies and Trusted Bodies. A more detailed summary of the prohibitions and relevant legislative provisions is provided in **Appendix 4**.

We make the following observations on these general prohibitions.

- The AER and AEMC must take all reasonable measures to protect data from unauthorised use or disclosure – this relates not just to confidential information, but any information obtained compulsorily (ie even if it is not confidential by its nature).
- AEMO's obligations are similar but limited to confidential information.
- However, for AEMO, the prohibitions specifically provide that (1) it makes unauthorised *use* of protected information if (and only if) it uses the information contrary to the Law, Rules or Regulations and (2) it makes an unauthorised *disclosure* of protected information if the disclosure is not authorised under the Law, Rules or Regulations (section 54(2) and (3) of the NEL and section 91G(2) and (3) of the NGL). This places a heavy onus on AEMO to identify an unqualified express right to use and share information.
- The prohibitions on the Trusted Bodies are often stricter than the Core Bodies. For example, the ABS has no right to release or share information other than by Ministerial determination. Further, there are secrecy offences which carry significant penalties for unauthorised disclosure of information given under the CS Act (see Table 2).
- As noted above, there are rational policy reasons for a default prohibition, but it does require the relevant bodies to identify an express right to use and share data and there may be an understandable inherent bias to conservatism in the interpretation of those rights. This is particularly so where it is necessary to interpret rights and prohibitions in legislation, Rules and Procedures which may not be consistent.

Table 1. Core Bodies

The general prohibitions against disclosure for Core Bodies are broad and there is a wide scope of information that can be considered "confidential".

<table>
<tr><th>AEMO</th><th>AER</th><th>AEMC</th></tr>
<tr><td>Must take all reasonable measures to protect "protected information" from unauthorised use or disclosure.

Protected information is:
given to AEMO in confidence; or
given to AEMO in connection with the performance of its statutory functions, and:
is stated under the statutory framework or by AEMO, the AER or the AEMC to be confidential, or
is otherwise confidential or commercially sensitive.
It also includes information which is derived from protected information.</td><td colspan="2">Must take all reasonable measures to protect from unauthorised use or disclosure information:
given to it in confidence in, or in connection with, the performance of its functions or the exercise of its powers; or
that is obtained by compulsion in the exercise of its powers.</td></tr>
<tr><td></td><td>AND

has further obligations regarding confidential information obtained from a wholesale electricity supplier for the purpose of wholesale market monitoring or reporting functions.</td><td>AND

information provided for the purposes of a Ministerial Council of Energy (MCE) directed review or an AEMC review is confidential information if:
the person who provides it claims, when providing it to the AEMC, that it is confidential information; and
the AEMC decides that the information is confidential information.
AND

there is a restriction on publishing any information in any written submission or comment if it is claimed as confidential, and if AEMC decides it is confidential.</td></tr>
</table>

Table 2. Trusted Bodies

The general prohibitions against data disclosure vary depending on the legislation governing each Trusted Body.

ACCC*	CER	ABS
Under s95ZN of the CCA, must not disclose information: ▪ made available, or to be made available (in oral evidence or in a document) at a hearing of an ACCC inquiry; or ▪ given or contained in a document produced by a person under s95ZK of the CCA; where a person claims that disclosure would damage their competitive position. **PROVIDED** where a person makes a claim that the disclosure would damage their competitive position, the ACCC is: ▪ satisfied that the claim is justified; and ▪ not of the opinion that disclosure is necessary in the public interest. There is also a **secrecy offence u**nder s95ZP of the CCA in relation to an "entrusted person", which is a current or former member or staff member of the ACCC, or a person appointed or engaged under the *Public Service Act 1999* (Cth). It is an offence for an entrusted person to disclose information outside the course of performing or exercising functions, powers or duties under or in relation to the CCA, if that information was disclosed to, or obtained by, that person for the purposes of Part VIIA of the CCA (Prices surveillance) and has not been made available to the public under Part VIIA of the CCA and	There is a **secrecy offence** in relation to: "**Protected information**", which is: ▪ obtained by a person in their capacity as an official of the CER; and ▪ disclosed by that person to another person or, used by the person.	Circumstances where a person is, or has been, the Statistician or an officer, and ▪ directly or indirectly divulges to another person (other than the person from whom the information was obtained) any information given under the CS Act; or ▪ gives an undertaking specified as a term or condition of a Ministerial determination providing for disclosure (or non-disclosure) of certain information, and fails to comply with the undertaking. **AND** non-disclosure obligations apply to Census information obtained by statisticians, which may not (in certain circumstances) be divulged to: ▪ a Department, Executive Agency or Statutory Agency; or ▪ a court or tribunal, whether compulsorily or voluntarily.

not contained in oral evidence given in public at the hearing of an inquiry.		

There is a **secrecy offence** if certain persons obtain and disclose "greenhouse and energy information" other than in accordance with the NGER. The offence applies to persons including authorised officers, audit team leaders or members (each as defined in the NGER Act), employees of the Commonwealth, States and Territories (or employees of an authority of the Commonwealth, a State or a Territory) and persons appointed to an office under a law of the Commonwealth, a State or a Territory.

"Greenhouse and energy information" is information reported to the CER or obtained while performing duties under the NGER Act.

*Note: There are other CCA provisions dealing with information obtained by the ACCC. Section 952N is particularly relevant to the energy sector given the ACCC's enquiries into electricity and gas under section 95H.

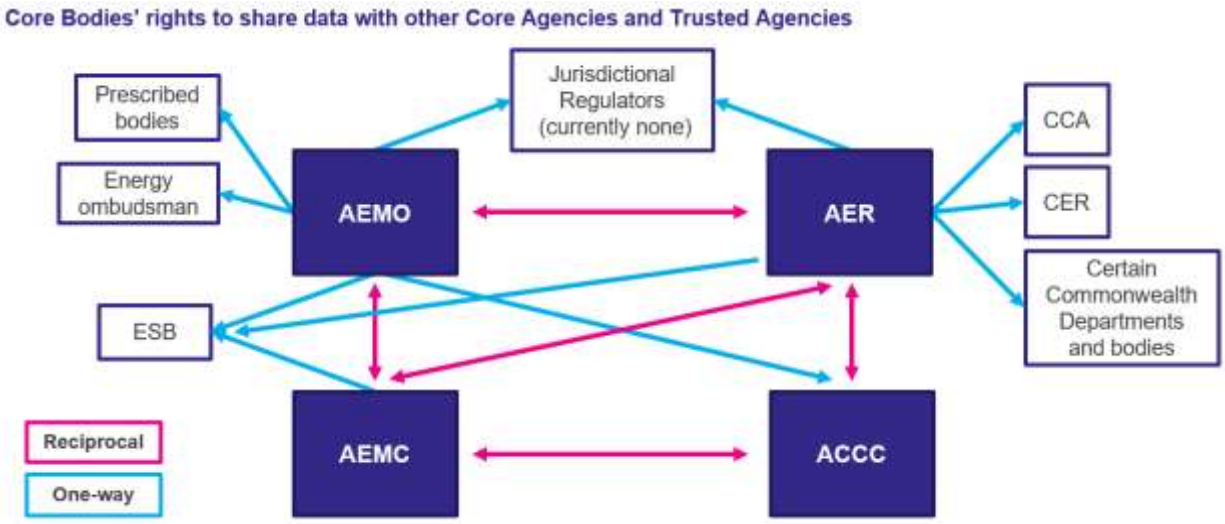
3 Authorised data sharing

Despite the above general prohibitions on data sharing, there are several broad principled exceptions within the relevant energy legislation that permit data sharing.

3.1 Permitted data sharing between Core Bodies and Trusted Bodies

Data may be shared by Core Bodies and Trusted Bodies to another Core Body or Trusted Body if the data is used by the recipient for purposes connected with the performance of its functions or exercise of its powers (summarised in the diagram below).

A Core Body or Trusted Body sharing this data may also impose conditions on the recipient's use or further sharing of that data.



Entity	Reference
AEMO	s54C NEL and s91GC NGL
AEMC	s24 AEMC Establishing Act
AER	s44AAF CCA (given effect by s30 NGL, s18 NEL), s28YA NEL, s326A of the NGL and ss210A of the NERL
ACCC	s157A CCA

Data may also be shared by Trusted Bodies in some other circumstances. For example, section 49 of the CER Act permits the Chair of the CER to authorise disclosure of certain information by an official of the CER to certain agencies or bodies (including the ABS, ACCC, AER, AEMO, ARENA, BOM or CSIRO) if the Chair of the CER is satisfied that the information will enable or assist that agency or body to perform or exercise any of the agency's or body's functions or powers. The Chair of the CER may impose conditions in relation to the information.

3.2 Permitted sharing with other bodies or release to the public at large

Where there is an overriding public interest in doing so (summarised in the table below), the energy legislation permits sharing with other bodies or release to the public at large. There are no restrictions in energy laws related to secondary use of that data.

Table 3. Rights to release data to the public at large

Body	Reference	Sharing or release right
AEMO	s54H NEL s91GH NGL	AEMO may disclose protected information if it: ▪ will not cause detriment to the person who gave the information or the person from whom it was received; or ▪ the **public benefit** in disclosing outweighs the detriment.
AER	s28ZB NEL s329 NGL s214 NERL	AER may disclose confidential information if it: ▪ will not cause detriment to the person who gave the information or the person from whom it was received; or ▪ the **public benefit** in disclosing outweighs the detriment.
ACCC	s95ZN CCA	Information given under a section 95ZK notice may be disclosed if the ACCC: ▪ is not satisfied the claim that disclosure will damage the person's competitive position is justified; or ▪ is of the opinion disclosure is necessary in the **public interest**.

3.3 Permitted data sharing in a range of other circumstances

The energy legislation provides for a number of other specific circumstances where energy market bodies are permitted to share data, including:

- where disclosure is required or authorised by law (AEMO, AEMC and the AER);
- with consent (AEMO and the AER);
- in de-identified or sufficiently aggregated form (AEMO and the AER, as well as a limited right for the CER to publish "greenhouse and energy information" under the NGER);
- if confidential information is omitted (AEMO, AEMC and the AER); and
- for the safety and proper operation of market (AEMO).

4 Broad use rights in energy laws

Our review of the energy laws found that data use restrictions are more commonly placed on secondary data usage (the use of data provided by another agency or body) rather than on data originally collected by an agency or body itself.

Most energy market bodies have a broad right to use data they collected for any purposes within their statutory functions.

Accordingly, while some use concerns were raised by Core Bodies in the RFI process, this appears to be by exception and limited to specific instances rather than a general problem or as a result of complying with use conditions imposed on the Core Bodies, particularly where information may be voluntarily provided.

4.1 AEMO

In the case of AEMO, this general power is established by section 53D of the NEL, which provides:

> **53D—Use of information**
>
> Subject to this Law, the Rules and the Regulations, AEMO may use information obtained by market information instrument or in any other way for any purpose connected with the exercise of any of its statutory functions.

The note in section 54 of the NEL makes it clear that section 53D is not limited in its operation to Division 5 of the NEL.

> **Note—**
>
> Section 53D authorises AEMO (subject to the Law, the Rules and the Regulations) to use information (whether obtained by market information instrument or in any other way) for any purpose connected with the exercise of any of its statutory functions.

Equivalent provisions are in the NGL at section 91FD and section 91G(2).

However, there are Rules that, depending on how they are interpreted, may narrow the broad use rights in relation to specific datasets, for example rule 7.11.1(f) of the NER:

> (f) The *settlements ready data* held in the *metering database* must be used by *AEMO* for *settlements* purposes.

4.2 AER

An exception to this pattern is the AER's use of data collected from wholesale electricity suppliers under section 18D(1)(b) of the NEL (partial extraction of s18D below).

18D—Provision, use and disclosure of information

(1) The following provisions apply to the performance of the AER wholesale market monitoring functions:

(a) the AER must, in performing the AER wholesale market monitoring functions in relation to a wholesale electricity market, use publicly available information to identify any relevant matter referred to in section 18C(1);

(b) if the AER has, in accordance with paragraph (a), identified any such relevant matter, the AER may, in accordance with its powers under this Part, obtain information from a wholesale electricity supplier—

(i) to assist it in determining whether—

(A) there is effective competition within the market; and

(B) there are features of the market that may be detrimental to effective competition within the market; and

(C) there are features of the market that may be impacting detrimentally on the efficient functioning of the market (and, if so, to assess the extent of the inefficiency); and

(ii) if there is an inefficiency identified, to analyse if the inefficiency gives rise to competition in the market that is not effective competition (or, in relation to an inefficiency identified by the AER but that is no longer present in the market, if the inefficiency gave rise to competition in the market that was not effective competition).

(2) Information obtained under subsection (1)(b) is taken to have been given to the AER in confidence (whether or not an express claim of confidentiality is made when the information is given).

(3) Despite anything to the contrary in this Part, the AER must not use confidential supplier information for any purpose other than the performance of the AER wholesale market monitoring functions or the AER wholesale market reporting functions.

(4) Despite anything to the contrary in this Part, the AER must not disclose confidential supplier information unless—

(a) the disclosure is for the purposes of the AER wholesale market monitoring functions or the AER wholesale market reporting functions; and

(b) the confidential supplier information has been combined or arranged with other information so that it does not reveal any confidential aspects of the confidential supplier information or identify the wholesale electricity supplier to whom the information relates.

The AER's own use of this data is limited to its wholesale market monitoring and reporting functions. This reflects a policy decision that the AER should not be able to use information gained by selective market monitoring for other, unrelated purposes.

5 Limitations on data sharing

Despite having broad statutory sharing rights, it is clear from the RFI process that Core Bodies face difficulties sharing data between themselves or with Trusted Bodies.

We have developed several hypotheses as to the reasons for this, which are discussed below.

5.1 Issue 1 – limited sharing rights

The scope of data sharing rights between energy market bodies is limited – that is, not every Core Body has an express right to share data with every other Core Body and some Trusted Bodies can't share information with other energy market bodies at all (see the diagram in section 3 of Part B above).

For example, the ACCC has no power to share data with AEMO, and the CER requires written authorisation by the Chair of the CER to share certain information with Core Bodies or other Trusted Bodies.

More specifically, four additional complexities arise.

Firstly, for the ACCC, the sharing permission in section 157A of the CCA (which would apply to information collected in respect of the electricity and gas market inquiries under section 95ZK) requires the ACCC to consider the receiving body's intended use of the data against that body's powers and functions:

> (1) The Commission or a Commission official may disclose to:
>
> (a) the AER; or
>
> (b) the AEMC; or
>
> (c) any staff or consultant assisting the AER or the AEMC in performing its functions or exercising its powers;
>
> any information that it obtains under this Act that is relevant to the functions or powers of the AER or the AEMC.

This requires an exercise of legal judgement as to whether the specific intended use of the data (as described by the data recipient) falls within the recipient's functions or powers. Although such functions and powers are clearly defined, reasonable minds may differ about the extent to which specific use cases fall within the general functions and powers. The consequences can be significant if the ACCC gets this wrong, so in the absence of a requirement to share information (as opposed to a discretionary right to share information), the ACCC may take a conservative view and not share data.

Further, the secrecy offence in section 95ZP of the CCA makes it an offence for an entrusted person (such as a member or staff member of the ACCC) to disclose "protected information" (being non-public information received under Part VIIA of the CCA) unless the person is acting in the course of performing or exercising functions, powers or duties under or in relation to this Act. As disclosure to the AER and AEMC is within the ACCC's powers, this provision does not restrict the ACCC or its staff members disclosing the protected information to those bodies. In the case of AEMO and other bodies, however, an ACCC officer must find a specific function, power or duty to lawfully disclose. Again, the consequences of getting this wrong can be significant. Secondly, for AEMO, the AER and AEMC, where sharing is authorised for other Core Bodies and certain other energy market bodies, the data seeker's own use of shared data is restricted to a purpose connected with the performance of the data seeker's functions or the exercise of the data seeker's powers (section 54C(3) of the NEL is an example which is representative of the issue). This may prompt the Core Body data-holder to

consider the data seeker's intended use of the data and whether conditions should be imposed, even though this is not a section that the Core Body itself is capable of breaching.

Reliance on the use of conditional disclosure may have resulted in unintended consequences for data sharing, such as:

- a lack of transparency for data seekers and the potential for inconsistent outcomes due to insufficient guidance on the appropriateness of conditions;
- placing more weight on the risks of sharing (the concerns of the data holder) over the benefits of sharing (the opportunities for the data seeker). As a data seeker is often unable to contest the conditions imposed, if the conditions are not acceptable to it, the only choice it has is not to access the data; and
- encouraging the use of bilateral data sharing agreements to allocate risk and liability for data sharing. However, contractual negotiations are often complex, time consuming and costly, which undermines efficient data sharing among energy market bodies and have issues relating to practicality and enforceability.

Thirdly, we understand it is not unusual for industry participants to prescribe information as confidential and not to be disclosed when they provide it to a Core Body. Particularly where the information is provided voluntarily or collected for a specific or narrow purpose, Core Bodies may consider themselves morally (if not legally) bound to comply with such express provisions which take precedence over general discretionary sharing rights.

Fourthly, there are specific restrictions on sharing in some cases. For example, for the AER, a specific exception to the AER's sharing power applies in relation to "confidential supplier information" under section 18D(4) of the NEL:

> (4) Despite anything to the contrary in this Part, the AER must not disclose confidential supplier information unless—
>
> (a) the disclosure is for the purposes of the AER wholesale market monitoring functions or the AER wholesale market reporting functions; and
>
> (b) the confidential supplier information has been combined or arranged with other information so that it does not reveal any confidential aspects of the confidential supplier information or identify the wholesale electricity supplier to whom the information relates.

However, this may be an appropriate policy outcome in relation to this data, which is considered highly sensitive.

5.2 Issue 2 – limited public benefit disclosure rights

Only AEMO, the AER and the ACCC have access to a public disclosure regime, as set out in Table 3 in section 3 above. Further, the public disclosure regimes are cumbersome and onerous on data holders (but not data seekers).

In the case of AEMO, it may disclose protected information if it is of the opinion:

- that the disclosure of the information would not cause detriment to the person who has given it or to a person from whom that person received it; or
- that although the disclosure of information would cause detriment to such a person, the public benefit in disclosing it outweighs that detriment (section 54H of the NEL).

Even if AEMO is satisfied in relation to one of the points above, before disclosing the protected information, AEMO must give both an "initial notice" and "further disclosure notice" to the person who gave AEMO the protected information, as well as to any "other" person who gave the first person the protected information (but only if AEMO is aware of that "other" person's identity and address). In most cases, even if all relevant persons could be identified, the administrative and cost burden of notifying each relevant person individually would be enough to deter AEMO from relying on this permission, particularly where AEMO is aware of a significant number of "other" persons. We summarise the extent of AEMO's obligations below.

1 In the first instance, AEMO is required to decide on the likely nature and extent of any detriment that may be caused and balance this against a public benefit that may be difficult to quantify or uncertain in respect of when or how it materialises. AEMO is required to do this in the absence of any guidance from the legislature as to what constitutes a public benefit or how to measure its likely impact.

2 Secondly, before disclosing the protected information, AEMO must give the person who gave the protected information a written notice stating that AEMO wishes to disclose the information and specifying the nature of the intended disclosure. The person must be invited to make submissions to AEMO against the disclosure of the protected information. In addition, if AEMO is aware that the person who gave the information in turn received it from another person, and AEMO is aware of that other person's identity and address, AEMO must give that other person a written notice and invite submissions.

3 Thirdly, if, after considering the representations, AEMO wishes to disclose the information, it must issue all relevant persons a further disclosure notice setting out why AEMO is of the opinion that the public benefit in disclosing outweighs the detriment the individual will suffer.

When added to the fact that the disclosure of the data could cause serious detriment and the body is under no obligation to disclose the data (ie this regime is discretionary), it is not surprising that AEMO has, to our knowledge, never relied on public disclosure rights.

The requirements on the AER are similar, although additional considerations are required for information given to the AER in compliance with a regulatory information instrument.

In addition to the resource intensity and time period required to obtain these permissions, there is real uncertainty about how these notice requirements apply where an body wishes to disclose a dynamic dataset on an ongoing basis, rather than make a discreet disclosure of a static dataset.

5.3 Issue 3 – complex interaction between Rules and law

While the above permissions for data sharing exist in the NEL, NGL, NERL and the AEMC Establishing Act, there is apparent uncertainty about how these permissions interact with specific and seemingly more limited data-related provisions in the Rules and guidelines.

While at the level of the NEL, NERL and NGL, the law remains relatively static, the NER, NERR and NGR are subject to frequent amendments. The rules have, therefore, naturally been used to clarify and particularise the rights in the NEL, NERL and NGL, including the Core Bodies' data collection rights.

For example, the NER has been amended to include specific data collection rights on the part of AEMO, despite there being grounds to argue that AEMO already possessed the requisite power to collect the data in question under the NEL. To provide clarity and reduce risk of challenge, these specific data collection rights are often linked to one of AEMO's powers or functions. For example,

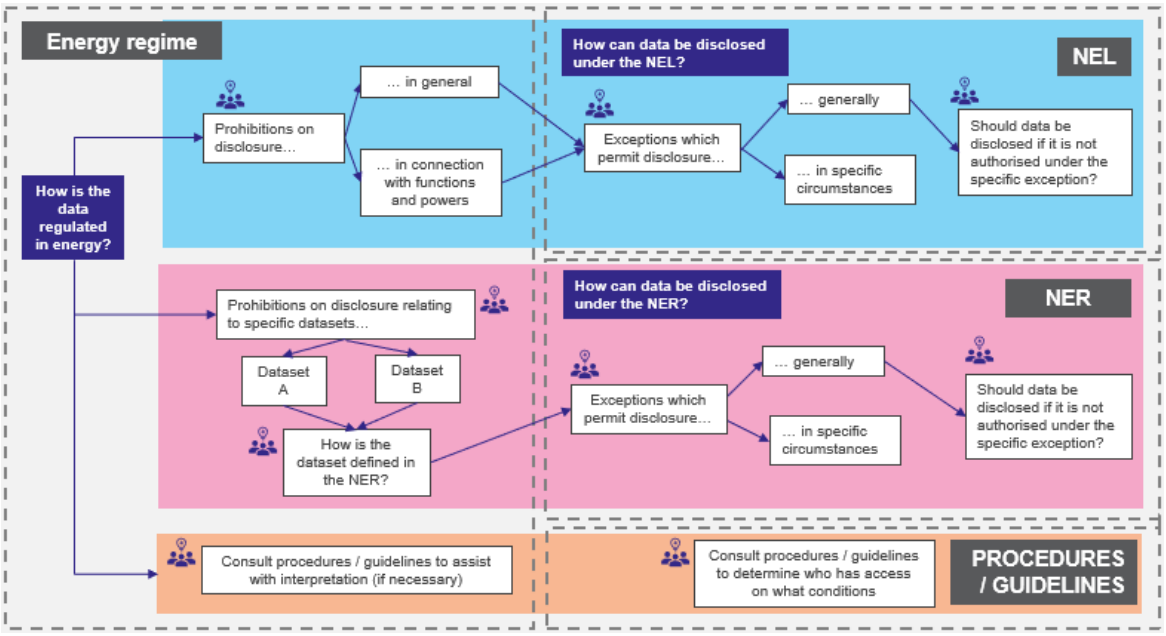
under the NER, Metering Data Providers must deliver metering data and relevant National Metering Identifier (**NMI**) Standing Data to AEMO "for settlements" (clause 7.10.1(a)(7)).

The consequence of this specificity in data collection rights in the rules, is that they may be interpreted as "reading down" the broad power of a Core Body to use the data for other purposes, or to share it with other Core Bodies that do not perform that particular function.

This tension between the general and the specific is not unique to energy data legislation. However, the lack of an overarching data strategy in the drafting of energy laws has created a complex web of interconnected clauses that may require a decision-maker to refer to multiple instruments to be able to discern whether data is shareable. In the context of the general prohibition on data sharing, this additional uncertainty creates risk for the decision maker.

A flow chart of the decisions a body may need to make when considering whether it can share data is provided below.

Flow chart 1. Hierarchy of decision making in the energy data regime



Accordingly, in the context of a general prohibition on data sharing, it is not surprising that concerns may arise that specific restrictions in the detailed rules and procedures, or the specific purpose of the collection power, limit data sharing or impose an obligation on the entity sharing the data to consider the use of that information by another entity.

5.4 Issue 4 – practical limitations

In addition to the above regulatory risks, energy market bodies face a range of practical limitations when attempting to share data, some of which are set out below.

- **Inconsistent systems –** there are many energy market bodies collecting data from a broad range of participants and yet, the energy sector lacks a body responsible for developing and maintaining data standards and interoperability frameworks. This means that energy market bodies' systems

are often incompatible, and datasets require significant investment in order to be made shareable and workable. AEMO's RFI response, for example, stated that analysts will generally avoid taking on work to obtain a workable dataset where there are considerable overheads.

- The DISER RFI response gave the example of the inconsistent approach to pricing information used by the AER, the AEMC, the ACCC and IPART, making the alignment of metrics challenging.
- The AER RFI response noted that although the AER is able to request metering data from AEMO, the mechanisms for the AER to receive the data using integrated systems (**APIs**) have not been available due to fragmented IT investment and capability.

- **Incomplete data –** where data systems are compatible, data quality issues may result in certain datasets being incomplete or incorrect in material respects. This stems from the fact that, currently, there is little incentive for a body to maintain high-quality datasets beyond its own immediate needs.
  - The AEMO RFI response gave the example of LV network connectivity data, held by DNSPs, with the completeness and accuracy of this data varying greatly across the businesses and jurisdictions.
  - The DISER RFI response gave the example of switching data, which captures some data that isn't switching and does not capture data that is switching.
- **Separation of electricity and gas –** despite the two energy types becoming increasingly interchangeable and a case being made for closer integration, separate data collection and maintenance systems exist for electricity and gas. However, the electricity and gas systems cannot be linked to form a complete view of the relevant data due to insufficient identification data for gas.
- **Cost allocation –** the energy industry lacks methods to allocate the cost of assessing a data request, processing the data into a shareable format and facilitating the data transfer. This acts as a significant disincentive where the cost/benefits are not shared equitably between energy market bodies.
  - The AEMO RFI response indicated that determining access limitations, extracting data and formatting it carries a resourcing cost to AEMO which it may not be able to bear, given constraints on its resources and its competing priorities.

6 Concerns about privacy

Fundamentally, privacy concerns can act as a deterrent to data sharing if data holders consider that they are unable to adequately manage the risks associated with data sharing in a way that protects the privacy interests of individuals. These privacy concerns arise out of the fact that the energy laws are not the only laws that regulate the protection of privacy of consumers in relation to energy data – the *Privacy Act 1998* (Cth) (**Privacy Act**) and State and Territory privacy legislation also apply to various participants in the energy sector.

This section 6:

- outlines the legislative framework that regulates the protection of privacy applicable to the energy sector (outside of the energy laws);
- discusses a threshold issue around what is "personal information" in the context of the energy sector, given privacy legislation protects the collection, use and disclosure of personal information;
- discusses the purposes for which personal information can be disclosed under the Privacy Act; and

- considers the way in which uses or disclosures of personal information under energy laws could be authorised uses or disclosures of that information under the Privacy Act.

6.1 The legislative framework regulating privacy

In relation to the Core Bodies operating within the energy sector, the following privacy regimes are relevant:

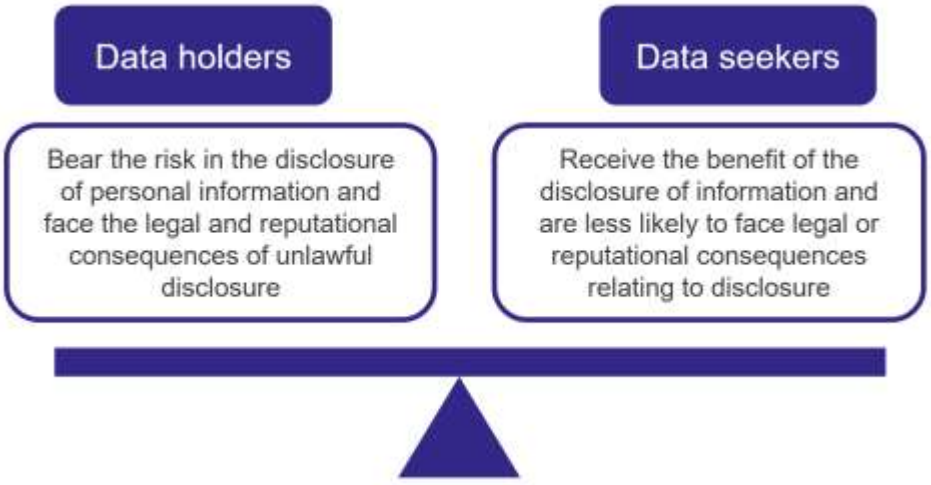
- the Privacy Act and the Australian Privacy Principles within the Privacy Act (APPs); and
- the privacy regimes of the States and Territories.

The Privacy Act and the APPs provide a framework for protecting, sharing and using "personal information" in Australia. The Privacy Act and APPs apply to Commonwealth "agencies" (such as the ABS, ACCC, AEMO, AER, ARENA, CER and CSIRO) and certain "organisations", including:

- individuals, bodies corporate, partnerships, unincorporated associations and trusts which meet the principles-based definition of "organisation" in the Privacy Act; and
- other organisations prescribed by the *Privacy Regulation 2013* (Cth) (such as Essential Energy, Ausgrid and Endeavour Energy).

The States and Territories have separate privacy regimes. However, this report focusses on the Commonwealth Privacy Act.

Australian privacy frameworks, including the Privacy Act as the most relevant, are principles-based regimes. Accordingly, legal interpretation and judgement are required when applying the principles, and the outcome of the application inevitably depends upon the context the decision maker operates within. For example, in the context of data sharing, principles-based privacy regimes create a tension between:



As a result, data holders are more likely to take a conservative view of the application of privacy principles to any disclosure of personal information than data seekers. This results in a tendency to not disclose data where uncertainty exists, such as in the absence of a clear legal right to disclose the data.

6.2 Determining if data is "personal information" and protected under privacy laws

Under the Privacy Act:

> ***personal information*** *means information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> *(a) whether the information or opinion is true or not; and*
>
> *(b) whether the information or opinion is recorded in a material form or not.*

For an individual to be "reasonably identifiable" by a person, the identity of the individual must be capable of being reasonably ascertained by that person from the information, or by combining the information with other information accessible by that person, taking into account the likelihood, cost, difficulty and practicality of that occurring.[1]

In the context of the energy sector, metering data is often a critical dataset that poses significant legal complexities when applying the definition of personal information. In determining whether metering data is personal information, there are a number of factors that data holders must consider before disclosing that information, including:

- **data held by third parties or in the public domain**: data may not be personal information in one entity's hands, but it can be personal information in a third party's hands if that third party has the ability to reasonably identify an individual by linking that data with information held by the third party or information in the public domain.

  Example

  We understand that AEMO is unlikely to be able to reasonably identify an individual from metering data held on the MSATS database (relevant datasets include individual NMIs, addresses and consumption data). This information alone, in the hands of AEMO (as the data holder), is unlikely to be "personal information" as significant costs and effort are required to make reidentification of individuals possible from that data.

  However, this same metering data in the hands of a retailer has the potential to be personal information if the retailer can reasonably identify individuals to whom the metering data relates. However, this may not always be the case as:

  - consumption data related to an individual NMI has the potential to be the personal information of multiple individuals (ie each individual living at the premises for that NMI) – is the data information about a single individual or is it information about a group of individuals? and
  - the accountholder details held by the retailer for the purposes of billing may not relate to those individuals consuming energy (ie accounts may be in the names of landlords, strata managers or parents) – is it possible to identify the individual to whom the information actually relates?
- **whether the data is susceptible to re-identification:** where datasets contain unique identifiers or patterns, associating the data with specific individuals through linking and decryption becomes easier, increasing the risk of re-identification; and
- **evolving technologies:** advances in technology and machine learning have decreased the cost and difficulty of re-identification through linking and decryption. This is particularly relevant to the disclosure of "real-time" data streams and consistent disclosure arrangements, where the risk of re-

[1] *Baptist Union of Queensland – Carinity v Roberts* [2015] FCA 1068.

identification must be continually assessed because disclosure is not bound by a single ”point-in-time”.

Given that Core Bodies that are data holders may not necessarily know what other information a data seeker could use to identify an individual, or what advanced technologies or techniques that a data seeker may use which would allow identification of an individual, when those Core Bodies receive a request for access to a data set they are more likely to take an approach that treats the data set as personal information and subject to the restrictions on disclosure in the Privacy Act.

Example

In 2019, Public Transport Victoria (PTV) released a dataset containing 1.8 billion historical records of public transport users' activity for use in the "Melbourne Datathon". The dataset contained the records of "touch on" and "touch off" activity of 15.1 million 'myki' cards used over a three-year period up to June 2018. In an effort to anonymise and de-identify the data, the actual myki numbers were not disclosed, but replaced by a meaningless number created by PTV.

Researchers were able to re-identify individuals using limited additional data points including their known public transport journeys. All trips during the three-year period using that card could then be linked to that individual. The Office of the Victorian Information Commissioner concluded that the datasets were personal information on the basis that the identity of a substantial proportion of the individuals whose travel movements were recorded in the dataset could reasonably be ascertained.

6.3 Relying on the primary purpose test or obtaining consent for a secondary purpose

Once a dataset is considered to be or contain "personal information" in the hands of a data seeker, then a data holder has to determine if the disclosure of the personal information to that data seeker is permitted under the Privacy Act. This will be the case if the disclosure is made:

- for the primary purpose for which it was collected; or
- for a secondary purpose, if:
  - the relevant person consents to the use or disclosure; or
  - broadly, the relevant person would reasonably expect the data holder to use or disclose that information for the secondary purpose and that secondary purpose is related to the primary purpose of collection.

6.4 Primary purpose

The primary purpose of collection of personal information is determined by reference to the purposes for which the data holder collected the personal information. In the case of energy data collected by Core Bodies, this could be construed:

- **narrowly**, by reference to specific collection rights under the Rules; or
- **broadly**, by reference to general collection powers under the legislation that relate to powers and functions.

Either construction is likely to limit disclosure to a third party where the intended use by the third party is not clearly within the scope of the disclosing Core Bodies' functions or powers or is inconsistent with the specific rule under which the information was originally collected. See section 5 above in relation to the tension between the general principles and the specific provisions in the energy laws and Rules.

6.5 Secondary purpose

Confusingly, in the energy sector, it is rare that Core Bodies directly collect data from consumers. That data is usually collected by market participants (such as retailers and metering data providers) and then provided to Core Bodies. In these circumstances, it is not clear in relation to the Core Bodies if the "primary purpose" of collection is determined by reference to the collection purposes of the retailer or the metering data provider, or if it is determined by reference to the collection purposes of the Core Bodies in performing their functions under the NEL and the Rules.

If the collection purpose is to be determined by reference to the collection by the retailer or metering data provider, then it would be difficult for Core Bodies to:

- be satisfied that individuals that are the subject of the data would have reasonably expected (or even contemplated) the secondary disclosure at the time the information was originally collected; or
- obtain consent from the relevant individuals, as Core Bodies:
  - do not have a direct relationship with the individuals that are the subject of the data and obtaining bulk consent (eg by way of Retail Standard Terms) has the risks of undermining the validity of such consent; and
  - may not be able to identify the individuals that are the subject of the data so as to obtain their consent (despite the fact that other data recipients may be able to use that data to identify an individual).

Considering this complexity, it is understandable that Core Bodies are hesitant to apply the secondary purpose test, or any existing consent mechanism, to authorise the disclosure of personal information. This is further exacerbated by the fact that the data holder is responsible for determining the nature and extent of both the primary and secondary purposes and bears the legal risk of a breach of privacy laws in connection with the disclosure.

6.6 Relying on the "required or authorised" by law exception to permit use or disclosure

Under the Privacy Act, a data holder may use or disclose personal information for a secondary purpose if the use or disclosure is required or authorised by an Australian law.

An "Australian law" includes:

- an Act of the Commonwealth or of a State or Territory;
- regulations, or any other instrument, made under such an Act; and
- a rule of common law or equity.

The NEL, the Rules, and regulations relevant to energy data each fall within the meaning of "Australian law" for the purposes of the Privacy Act.

As identified in section 3 of Part B, there are a number of broad and specific provisions in the energy legislation and Rules that "require" or "authorise" the disclosure of personal information from Core Bodies to other Core Bodies, Trusted Bodies and other third parties for a secondary purpose. However, energy market bodies may have concerns about the validity of authorisations or permissions under law. This may be problematic where the authorisation or permission is open to interpretation or where legal uncertainty exists, for example:

- limited authorisation for the disclosure of aggregated or non-identifying information by AEMO (sections 54F and 54FA of the NEL) and the AER (sections 28ZA and 28ZAA of the NEL). However, such disclosure is limited to those two energy market bodies and does not absolve

AEMO or the AER of re-identification risk, which requires both a legal and technical view on the extent to which the data has been anonymised and whether an individual may still be reasonably identified from the data. Further, in the event that data is released or shared and is then re-identified (as described in the PTV example above), privacy laws will still apply, and these provisions do nothing to mitigate the residual reputational risk which arises as a function of being a custodian of personal information; and

- references in the law which expressly apply the relevant privacy principles (including the restrictions on disclosure) despite a corresponding authorisation or requirement to disclose information, for example, rule 3.7E of the NER provides:

> (l) *AEMO* must prepare and publish on its website a report of aggregated *DER register information* (*DER register report*) in accordance with the *DER register information guidelines*.
>
> and:
>
> (r) Nothing in this rule 3.7E:
>
> (1) requires *AEMO* to make available *DER register information* where the collection, use or disclosure of that information by *AEMO* would breach applicable privacy laws; or

It is clear from this that the interaction between the Rules and the Privacy Act has been considered during the rule making process. There is a question as to how the Rule making process for a particular Rule change should apply and address broader public benefits for the sharing of data resulting from that Rule change, particularly when that public benefit (considered on a longer-term basis) may not be an immediate focus of the particular Rule change.

It is important to note that while a data holder may be able to rely on a "required or authorised by law" exception, to the extent that it still holds personal information, it will still be subject to obligations under the Privacy Act in respect of that personal information (eg the obligation in APP 11 to take reasonable steps to protect the security of personal information that it holds).

Even if a Core Body is comfortable that the disclosure would clearly fall within the "authorised or required" by law exception, the lack of guidance or certainty for mitigation of commercial, reputational and ethical risks associated with privacy issues may result in a reluctance to disclose (given the Privacy Act does not mandate disclosure).

The CDR regime, recently enacted as a new Part IVD of the CCA, is structured to take advantage of the "authorised or required" by law exception to the Privacy Act, making all disclosures of CDR data under the regime "required" or "permitted" by law. However, the CDR framework provides a clear regime for managing risks associated with privacy outside the privacy law framework through the application of privacy safeguards set out in sections 56ED to 56EP of the CCA. For example, section 56EC of the CCA ("relationship with other laws") provides:

(4) Despite the *Privacy Act 1988*:

(a) the Australian Privacy Principles do not apply to an accredited data recipient of CDR data in relation to the CDR data; and

(b) if subsection 56EN(1) applies to a disclosure of CDR data by a data holder of the CDR data—Australian Privacy Principle 10 does not apply to the data holder in relation to that disclosure of the CDR data; and

(c) if subsection 56EP(1) applies to CDR data and a data holder of the CDR data—Australian Privacy Principle 13 does not apply to the data holder in relation to the CDR data; and

(d) Australian Privacy Principles 6, 7 and 11 do not apply to a designated gateway for CDR data in relation to the CDR data.

Note 1: For the accredited data recipient, the privacy safeguards will apply instead.

Note 2: Section 56EN (or privacy safeguard 11) is about the quality of CDR data. Section 56EP (or privacy safeguard 13) is about correcting CDR data.

(5) Apart from paragraphs (4)(b) to (d), this Division does not affect how the Australian Privacy Principles apply to:

(a) a data holder of CDR data in relation to the CDR data; or

(b) a designated gateway for CDR data in relation to the CDR data.

Note 1: Privacy safeguard 1 will apply to a data holder or designated gateway in parallel to Australian Privacy Principle 1.

Note 2: The consumer data rules (which are made under Division 2) will affect how the Australian Privacy Principles apply. Requirements and authorisations under those rules will be requirements or authorisations under an Australian law for the purposes of the Australian Privacy Principles.

Faced with these residual risks and legal uncertainties, it is understandable that data holders may, to the extent permitted by law,[2] choose to take a conservative approach by withholding data or imposing additional contractual restrictions on the data seeker, particularly where it is possible that the use of the information by the data seeker could interfere with the privacy of affected individuals.

[2] We note that Rule 4.6(4) of the *Competition and Consumer (Consumer Data Right) Rules 2020* requires data holders to disclose CDR Data in response to a consumer request.

7 Concerns about confidentiality

Concerns about breaching confidentiality is a further barrier to data sharing that needs to be overcome. Much of the data held by Core Bodies collected from energy market participants is likely to be subject to obligations of confidence which arise as follows:

Statute

The current legislative regime prohibits use and sharing of a broad range of information that is collected by Core Agencies, as identified in section 2 of Part B above.

Contract

Market Participants utilise contractual restrictions when disclosing data to Core Agencies and these restrictions may act to exclude secondary disclosure by limiting the data holder's use of the data to the narrow purpose for which the data was collected. Data sharing agreements and confidentiality undertakings between Core Agencies and with other Trusted Agencies may also restrict use and sharing of confidential information.

Equity

An equitable action for breach of confidence arises if:

- information possesses the quality of confidence;
- the information was imparted in circumstances giving rise to an obligation of confidence; and
- there was an unauthorised use (not merely disclosure) of the confidential information to the detriment of the party communicating it.

This section 7 of Part B focuses on confidentiality obligations arising under contract or in equity. Section 2 of Part B (above) considered confidentiality obligations arising under energy laws.

Where obligations of confidence limit use and sharing of data, a clear legislative provision requiring sharing (or in some cases, authorising sharing) can override contractual or equitable obligations of confidence.

7.1 Disclosures "required" by law

An unambiguous statutory requirement to disclose information will override the general statutory prohibitions on, and presumptions against, disclosure as well as any contractual or equitable obligations of confidentiality.

For example, clause 2A.5.2 of the NER and rule 26 of the NGL provide:

2A.5.2 AEMC may direct AEMO to provide information

(a) Where the *AEMC*:

(1) directs an applicant or an alternative proponent to provide supplementary economic analysis under clause 2A.5.1; or

(2) decides that it or its *representative* will prepare supplementary economic analysis under clause 2A.5.1(e),

the *AEMC* may request *AEMO* to provide information (including *constraint* equations) to the applicant or to the alternative proponent, or directly to the *AEMC* (as the case may be), but only where such information is necessary to facilitate the provision of supplementary economic analysis to those persons or to the *AEMC*.

(b) Where the *AEMC* requests *AEMO* to provide information under paragraph (a), *AEMO* must provide the information to the applicant, to the alternative proponent, or directly to the *AEMC* (as the case may be), as soon as practicable in all the circumstances.

26 Classification of tender approval pipeline

(1) When the *tender approval decision* becomes irrevocable:

(a) the proposed pipeline described in the successful tender selected in accordance with the approved process becomes a *CTP pipeline*; and

(b) the AER must ask the NCC to classify the pipeline in accordance with the pipeline classification criterion.

(2) The AER must provide the NCC with information the NCC reasonably requires to classify the pipeline.

7.2 Disclosures "authorised" or "permitted" by law

It is less clear that a statutory provision that merely "authorises" or "permits" disclosure by a data holder will override a contractual or equitable obligation of confidence. This is because the data holder is not obliged to make the disclosure but has a choice to make or not make the disclosure. If it chooses to make the disclosure, then it also has to accept the consequences of doing so, which could include liability for breach of confidence.

For example, the exceptions to the general confidentiality regime in the NEL are constructed as "authorisations", such as section 28X:

> **28X—Disclosure with prior written consent is authorised**
>
> The AER is authorised to disclose information given to it in confidence if the AER has the written consent to do so of—
>
> (a) the person who gave the information; or
>
> (b) the person from whom the person referred to in paragraph (a) received that information.

As a result, Core Bodies are likely to be reluctant to rely on authorisations or discretionary permissions to disclose confidential information. This reluctance may explain the trend towards prescription in the Rules, mandating the disclosure of particular datasets by Core Bodies.

7.3 Expectations of confidence

One final consideration relates to whether information collected by government entities should be used or shared, even if obligations of confidence do not apply. The question is, just because a Core Body can use or share data, should it?

Where there is only an expectation from a private sector entity that provides data to a government entity that the information will be used for the limited purpose for which it was provided, without a legal obligation of confidence, government entities should consider:

- the public benefit related to the disclosure of the relevant information; and
- whether sharing of the information may disincentivise the data provider from providing information on a voluntary basis in the future.

8 Risk and liability gaps

The final barrier discussed in this report that we think hinders data sharing in the energy sector is the liability of the data holder to third parties arising out of shared data.

Risk could arise in relation to liability to:

- the **data seeker**, for loss or harm incurred as a result of the provision by the data holder of inaccurate or incomplete data, or data that results in a breach of a third party's rights (including an interference with their privacy). This is particularly problematic as data held by Core Bodies has often been collected from market participants or has been compiled from third party sources on an 'as-is' basis. While market participants are required to provide accurate, sufficient and complete data at the time of collection (for example see clauses 3.13.13 and 3.8.22A of the NER) and also provide statutory indemnities (see below), these protections are not sufficient to protect the data holder from all claims;
- **subsequent data recipients**, who receive the information (or information derived from the information) from the data seeker, who use and rely on it to their detriment (eg if the information is inaccurate) and then seek to take action against the data holder; and
- **affected individuals**, who consider that their privacy or other rights have been interfered with.

Faced with these risks, it is understandable that a data holder would want to ensure that sharing of data does not give rise to any risk exposure, particularly if the data holder receives no particular benefit from sharing the data.

While in a commercial context, this type of risk allocation is typically dealt with through the use of exclusions or limitations of liability, warranties and indemnities, these mechanisms are not appropriate for Core Bodies as:

- exclusions or limitations of liability only work between the parties to a contract or deed, and do not bind third parties or underlying individuals; and
- Core Bodies may not have the power to give indemnities or may be subject to policies that effectively restrict them from giving indemnities.

Finally, the immunities and indemnities provided to Core Bodies in the current energy regime that may protect them from this risk exposure, though broad, may not be considered to offer enough protection for a Core Body that wishes to share data. For example:

Table 4. Immunities and indemnities

Body	Reference	Finding
AEMO	s119 NEL	First, this immunity only relates to actions or omissions in performance of AEMO's own functions and powers. The data sharing would need to be able to be clearly characterised as a function or power of AEMO for this immunity to apply. Second, the immunity does not apply to negligence (although liability is capped). Accordingly, a disclosure of confidential information where authorised but AEMO has not taken reasonable care to protect the information in the circumstances could arguably not be subject to the immunity.
AER	s18E NEL	First, the AER's immunity is limited to confidential supplier information, being information obtained from a wholesale electricity supplier under section 18D(1)(b) of the NEL that is taken to be confidential information under section 18D(2) of the NEL. Second, this immunity is only applicable in certain circumstances (ie if the AER reasonably believed the information was not confidential, or that the information would not reveal confidential aspects of the information or identify a wholesale electricity supplier to whom the information relates).
AEMC	s121 NEL and s18 AEMC EA	The AEMC's immunity only relates to officials, the Commissioner or AEMC staff and not the AEMC. The immunity is also not appropriate for data sharing as it is limited to actions in performance of AEMC's own functions and powers.

AER, AEMC and AEMO	r8.6.5 NER	This rule requires each Registered Participant to indemnify the AER, AEMC and AEMO against any claim, action, damage, loss, liability, expense or outgoing which the AER, the AEMC or AEMO pays, suffers, incurs or is liable for in respect of any breach by that Registered Participant of r8.6, which covers (at a high-level) keeping confidential information confidential; the disclosure of confidential information; the reproduction of confidential information and access to confidential information. The indemnity does not apply to data sharing between public bodies.

The net result of this is that any data sharing model must address risk and liability in a sensible and practicable way for that model to have any likelihood of success.

C. Approaches to data regulation in other sectors and internationally

1 Approaches to data regulation in other sectors in Australia

In this section we examine several local data sharing initiatives that may provide lessons for the energy sector. We have included examples from the health and telecommunications sectors (where data sharing is based on more of an ad-hoc approach) alongside the more comprehensive data sharing frameworks proposed under the CDR regime and the proposed DAT Act.

Table 5: Data sharing in other sectors

Data Sharing Initiatives	Brief description of regime for data sharing	Indication of principles or rules-based regime	Incorporation of privacy or other associated data regulations	How was it implemented and enforced?
A. CDR – Consumer Data Right	The CDR[3] is a customer driven initiative with a focus on data mobility. However, it is also likely to facilitate broader data sharing as participants implement common data standards. CDR is initially being applied in the banking sector, with energy and telecommunications data scheduled to follow.	Although the language of CDR implementation is based on 'rules' and 'standards' the overall approach is partly principles based. For example, a key principle is the data minimisation principle contained in the CDR Rules which can be summarised as: *accredited parties may only collect and use CDR data they reasonably need in order to provide goods or services in accordance with a request from a CDR consumer.*	CDR is being implemented in a coordinated approach, involving the: ▪ ACCC; ▪ OAIC; and ▪ Data Standards Body (**DSB**) – currently being co-ordinated by CSIRO/Data61. The CDR regime is set out in Part IVD of the *Competition and Consumer* Act 2010 (Cth) (**CCA**). The CCA contains the Privacy Safeguards that cover similar protections to those that apply to the handling of personal information under the Privacy Act and the Australian Privacy Principles. However, in some instances, the CDR privacy safeguards expand on these protections. For example, there is no equivalent APP for CDR Privacy Safeguard 10, which requires an accredited data recipient to notify the consumer when they disclose data. OAIC has released CDR Privacy Safeguard	CDR was initially enabled through the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth). CDR has initially been applied to the banking sector, but it will be rolled out to other sectors in phases. The current CDR Rules contain some specific measures for the banking sector. Measures for the energy sector are now being developed and it the energy sector will be the next sector covered by CDR. The CDR regime relies heavily on an accreditation process, including a 'fit and proper' person test. As the regime is being introduced under the ACCC's legislation, non-compliance carries severe penalties.

[3] <www.accc.gov.au/focus-areas/consumer-data-right-cdr-0>

			Guidelines outlining how it intends to apply the safeguards and exercise its powers and functions. These guidelines set not only the OAIC's view on minimum standards for compliance, but also examples of good privacy practice to supplement those standards.	

Data Sharing Initiatives	Brief description of regime for data sharing	Indication of principles or rules-based regime	Incorporation of privacy or other associated data regulations	How was it implemented and enforced?
B. DAT – Data Availability and Transparency Act (Cth) (forthcoming)	DAT[4] is based on comprehensive Commonwealth legislation that will allow data sharing requests to over-ride current secrecy and confidentiality provisions in other laws, subject to certain conditions. The proposal is initially limited to Commonwealth data but the ONDC has a long term goal to build towards a national system covering State and Territory data. The options for allowing other jurisdictions to be covered by the regime have not yet been released.	DAT is largely principles based, although some key rules are set out in detail. Meeting a high level 'purpose' test is the key requirement. The purpose test is prescriptive in that it provides strict limits on the use of shared data. The purpose test is complemented by 5 new data sharing principles[5] (based on the Five Safes framework). These principles are much more flexible in nature and each principle can be applied on a 'sliding scale' based on risk.	Some Privacy Act requirements remain in place, but they are largely replaced by specific requirements in DAT. These include: ▪ a data minimisation requirement; ▪ new data sharing principles (based on the Five Safes framework); ▪ a restriction on onward disclosure; and ▪ an accreditation scheme for access to the data. There is also a proposed list of prohibited purposes which may have a significant impact on data sharing. For example, prohibited purposes might include law enforcement, compliance and direct marketing.	The data sharing regime will be implemented by a mix of legislation and guidance from the new regulator – the National Data Commissioner. The National Data Commissioner will build trust in the system by accrediting users and data service providers to participate in the data sharing scheme. Accreditation will standardise and streamline existing processes. There are three criteria for accrediting users: 1. skills and capability to protect, manage and use data; 2. privacy standards if handling personal information; and 3. effective governance to manage and use data. An Exposure Draft of the proposed Bill is expected to be released for public consultation in late 2020.

4 <www.datacommissioner.gov.au/resources/discussion-paper>

5 <www.datacommissioner.gov.au/safeguards/sharing-principles> and <www.datacommissioner.gov.au/resources/sharing-data-safely-package>

Data Sharing Initiatives	Brief description of regime for data sharing	Indication of principles or rules-based regime	Incorporation of privacy or other associated data regulations	How was it implemented and enforced?
C. Health	There is no single framework for sharing health data in Australia. Instead, a variety of regulated 'channels' have developed to allow data sharing, subject to conditions. These range from data sharing arrangements under Privacy Act guidelines (eg for health research) to special legislative arrangements for sharing health provider information. It is important to note that there are significant restrictions on sharing some health data – for example the personal information held in the My Health Record data set is subject to a Secondary Use Framework that prohibits commercial access and use of the data by insurance companies. It also prohibits use of the data for assessing eligibility for benefits or individual compliance.[6]	A wide variety of sharing mechanisms exist, ranging from broad principles in the Privacy Act guidelines on sharing health data for research, to strict prohibitions on sharing (or matching) specific data sets, such as the My Health Record Data set. In general, the Privacy Act guidelines are principles based and attempt to facilitate data sharing subject to a broad set of risk management considerations.	Some data sharing in the health sector relies on guidelines issued by the OAIC that allow data to be shared as an exception to the APPs in the Privacy Act. Another common sharing mechanism is for Ministers (or their delegates) to issue Public Interest Certificates to allow data sharing as an additional form of Privacy Act exemption. In some rare cases data sharing is specifically permitted in health legislation, for example the recent *Health Legislation Amendment (Data-matching and Other Matters) Act 2019* (Cth).[7] In that Act a set of six specific 'permitted purposes' is set out for data matching. In all these examples, a breach of the conditions for data sharing (eg the permitted purposes) results in a breach of the Privacy Act (because the exemption being relied upon no longer applies).	Health data sharing occurs on an ad hoc basis, but is often implemented via specialist, accredited data integrators in the health or statistics field, eg the Sax Institute, the Australian Institute for Health and Welfare (AIHW) and the ABS. Some data sharing also occurs 'in house', eg at the Department of Health or at the Department of Human Services.

6 <www.myhealthrecord.gov.au/sites/default/files/secondary_use_of_data_fact_sheet.pdf?v=1537415418>

7 <consultations.health.gov.au/provider-benefits-integrity/draft-health-legislation-amendment-data-matching-b>

Data Sharing Initiatives	Brief description of regime for data sharing	Indication of principles or rules-based regime	Incorporation of privacy or other associated data regulations	How was it implemented and enforced?
D. Tele-communications	In Australia the telecommunications industry shares data under a system of industry Codes and Standards.[8] The sector will also be impacted by the CDR reforms (see above) in a later phase of implementation. An example of a relevant Code is the *Integrated Public Number Database Code 2017* (IPND). This Code sets out who can provide data to and/or use data from the IPND, and the rules for how they use that data. This data set was initially developed to facilitate service delivery, but has attracted wider interest over time (from researchers, law enforcement and other Government agencies).	The Codes tend to be quite prescriptive, although the overarching legislative framework is more principles based. The industry is often left to develop its own practices until a specific issue emerges (eg through customer complaints) and then the industry will respond with a Code. It is one of the few industry sectors in Australia which has a mature self-regulation framework of this type.	Privacy provisions are scattered throughout the Codes, and tend to be customised to the specific issue covered by that Code. The general approach is to set out conditions in which data can be shared in compliance with the *Telecommunications Act 1997* (Cth). Part 13 of that Act places restrictions on the disclosure of personal information, but numerous exemptions are available. The Codes help the industry to navigate the appropriate exemptions. For example, sections 285 and 285A of the Act allow data to be disclosed for information held in the IPND in some circumstances, and these are further elaborated on in the IPND Code.	Failure to comply with an industry Code may ultimately result in a breach of the *Telecommunications Act 1997* (Cth), so significant sanctions and penalties may apply. In practice the industry consists of licensed participants, so a threat to the licence acts as a deterrent to non-compliance with Codes and standards.

[8] <www.acma.gov.au/industry-codes-and-standards-telcos> and <www.commsalliance.com.au/Documents/all>

2 International data sharing initiatives

In this section we examine several international data sharing initiatives that have a direct impact on the energy sector. We have included examples that cover a wide spectrum, including the light touch approaches implemented in Singapore and the United States, and more robust approaches implemented (and proposed) in the Netherlands and the United Kingdom. The section is followed by a discussion of the key lessons from these case studies.

Table 6. International data sharing initiatives

Jurisdiction	Data sharing initiative	General approach	Privacy measures	Implementation
E. The Netherlands – Data Hub	The Netherlands Energy Data Hub (or Energie Data Services Nederland – EDSN)[9] was established in 2007 and has gradually become a central repository and clearinghouse for energy data. Current services include: ▪ customer portal giving customers control over their own data; ▪ central service to store and exchange structural data on both centralised and distributed power-generating facilities; and ▪ centralised and uniform allocation and reconciliation processes.	The Netherlands has adopted a centralised approach, where a single data service has been established to collect data from a variety of sources and then make integrated data sets available to interested parties.	The Netherlands operates within the EU General Data Protection Regulation (**GDPR**) context so all data sharing is subject to strict, prescriptive controls. Although the GDPR is written as a set of Principles it is in practice highly prescriptive. The most relevant sections are Article 5 and Article 6. Article 5 includes a number of key requirements for collecting and processing data, including: ▪ data must be processed lawfully, fairly and in a transparent manner; ▪ data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; and ▪ data must be adequate, relevant and limited to what is necessary. Article 6 includes an additional test of the lawful basis for use of data. Each use of personal data in the energy sector must therefore be justified by reference to an appropriate basis for processing (this might include research, planning and service delivery).	EDSN is a membership-based organisation that uses a mix of government funding and member contributions to develop industry wide standards, data catalogues and cloud based data sharing infrastructure.

[9] <www.edsn.nl/english>

Jurisdiction	Data sharing initiative	General approach	Privacy measures	Implementation
F. Singapore – EMA	Specific energy data initiatives are managed by the Singapore Energy Market Authority (EMA) <www.ema.gov.sg>.[10] They include a mix of traditional data hubs and publications, and more innovative use of technologies – including blockchain and AI.	The Singapore approach is very high level, principles based and light touch. Participation in the new data sharing initiatives is voluntary, and there is a strong focus on promoting innovation.	Singapore has light touch privacy legislation in place, but only for the private sector.	Energy data initiatives in Singapore are based on innovative technology, including blockchain and AI solutions.[11]
G. Singapore – Trusted Data Sharing Framework	In 2019 the Singapore Infocomm Media Development Authority (IMDA) <www.imda.gov.sg> issued the Trusted Data Sharing Framework[12] – a broad data sharing framework for all sectors.	The Framework aims to guide organisations through the 'data sharing journey' and outlines key considerations for organisations to take into account when planning data partnerships. It is very high level, principles based, voluntary and informative. The Framework is for guidance only and is not legally binding.	Singapore passed the Personal Data Protection (PDP) Act in October 2012. The legislation covers all of the private sector. It does not cover government agencies. The Personal Data Protection Commission (PDPC) <www.pdpc.gov.sg> oversees the legislation. The Trusted Data Sharing Framework advises organisations to seek advice on complying with the PDP Act, but provides no specific guidance.	This Framework is simply a set of voluntary guidelines and checklists.

10 <www.ema.gov.sg/Singapore_Energy_Statistics.aspx>

11 For example, see the use of blockchain technology by SP Group for renewable energy certificates: <www.spgroup.com.sg/what-we-do/sustainability-and-innovation/rec>

12 <www.imda.gov.sg/AI-and-Data> and <www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf>

Jurisdiction	Data sharing initiative	General approach	Privacy measures	Implementation
H. UK – NEED	The National Energy Efficiency Data Framework (NEED)[13] is a broad framework for energy data sharing and draws together a wide variety of data sources so that integrated data outputs can be developed.	NEED is moving from a rules-based approach to a principles based approach (slowly). However, this change is limited by the application of the GDPR which includes a number of prescriptive requirements and checks.	NEED operates within the constraints of the GDPR – so all data sharing involving personal information is subject to strict, prescriptive controls or relies on exemptions. NEED provides a simple way of accessing data in one spot, but behind the scenes the process of collecting data is extremely complex, with some similarities with the Australian market. NEED has to rely on a variety of legal instruments to access data. Examples include: ▪ Statistics of Trade Act 1947 ▪ Electricity Act 1989 ▪ Energy Performance of Buildings (England and Wales) Regulation 2012. Other data is purchased under contract or obtained from open data sources. NEED is subject to regular Privacy Impact Assessments – the latest was conducted in 2019.[14]	The NEED data hub is a simplified front end – hiding significant legal complexity behind the scenes. External users require accreditation, and some data can only be accessed on secure premises. Other low risk data sets are released as open data.

13 <data.gov.uk/dataset/473afefd-9028-48d1-a959-c865c1387a9d/national-energy-efficiency-data-framework-need>

14 <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/843490/need-data-framework-2019-privacy-impact-assessment.pdf>

Jurisdiction	Data sharing initiative	General approach	Privacy measures	Implementation
I. **UK – Smart Metering Framework**	Smart Metering Data Access and Privacy Framework.[15]	The Framework determines the levels of access to energy consumption data from smart meters for energy suppliers, network operators and third parties. It also establishes the purposes for which data can be collected and the choices available to consumers.	The central principle of the Framework is that consumers have control over who can access their energy consumption data, how often and for what purposes, except where this is required for regulated purposes. Consent plays a significant role, especially for more granular data. Explicit consent is required for any use of the data related to direct marketing. The consent provisions are complemented by an accreditation scheme for third party access to the data (eg organisations outside the energy sector).	The Data Access and Privacy Framework is a customer directed model, similar to the CDR regime in Australia. Energy providers and network operators have direct access to the data, subject to the consent requirements. Access by third parties is facilitated by an accreditation scheme. A 2018 review of the scheme concluded that it was too early to tell if the data accessed via the Framework was delivering public benefits.[16]

15 <www.gov.uk/government/consultations/smart-meter-data-access-and-privacy>

16 <www.gov.uk/government/publications/smart-metering-implementation-programme-review-of-the-data-access-and-privacy-framework>

Jurisdiction	Data sharing initiative	General approach	Privacy measures	Implementation
J. UK – Energy Data Taskforce	The Energy Data Taskforce[17] published A Strategy for a Modern Digitalised Energy System in mid-2019.[18] The report identified a range of barriers to data sharing in the UK energy sector and includes recommendations to remove these barriers.	The Taskforce recommendations are an ambitious and radical approach to sharing energy data, and the recommendations are being considered by Ofgem <www.ofgem.gov.uk> – the national energy regulator. Ofgem have indicated that they are likely to accept the report recommendations.[19]	The Taskforce strategy includes a significant move to a principles-based approach in the new framework. The key reform is that all energy data is 'presumed open': *Government and Ofgem should direct the sector to adopt the principle that Energy System Data should be Presumed Open, using their range of existing legislative and regulatory measures as appropriate, supported by requirements that data is 'Discoverable, Searchable, Understandable', with common 'Structures, Interfaces and Standards' and is 'Secure and Resilient'.* The strategy represents a response to years of frustration with the slow pace and high cost of providing access to energy data through existing mechanisms such as NEED (see above).	The new Framework includes key recommendations to establish: ▪ an energy data catalogue; ▪ an open data 'triage' process; and ▪ a registration process for access seekers (this appears to fall short of a full vetting / accreditation process). In October 2019 Ofgem, the Department for Business, Energy and Industrial Strategy and Innovate UK offered £1.9m in funding to develop a software platform to implement some of the key Taskforce plans, including software to facilitate access to energy datasets.

17 <www.gov.uk/government/groups/energy-data-taskforce>

18 <es.catapult.org.uk/news/energy-data-taskforce-report>

19 <www.ofgem.gov.uk/publications-and-updates/delivering-energy-data-taskforce-recommendations>

Jurisdiction	Data sharing initiative	General approach	Privacy measures	Implementation
K. USA – DataGuard	The US has a voluntary Code of Conduct in place – known as the DataGuard Energy Data Privacy Program (DataGuard).[20] The code provides energy companies with a consumer-facing mechanism for demonstrating their commitment to protecting consumers' data.	The US approach is principles based. It provides a very light touch, voluntary standards driven framework. The DataGuard principles are: ▪ Consumer Notice and Awareness ▪ Customer Choice and Consent ▪ Customer Data Access and Participation ▪ Integrity and Security ▪ Self-Enforcement Management and Redress	There is no single federal privacy law in the United States. A range of specific, sectoral laws impose privacy obligations in specific circumstances, along with state laws and regulations. Privacy protection in the health sector and the financial services sector are both strong. Only light touch privacy rules are in place in the energy sector, based on a competition and consumer protection model. Providers make a privacy 'promise' and stick to it. Enforcement only occurs for false and misleading conduct (ie when a promise is broken).	The US regulator provides a platform for some energy data assets, but the overall approach is loose and distributed, with a focus on innovation.[21] Interestingly there is also some customer driven innovation, with examples of consumers forming collectives to share anonymous energy data in order to improve services and access better pricing.[22]

20 <www.dataguardprivacyprogram.org/Program_Principles.html>

21 Refer to <exergy.energy> for an example of innovation in the sector.

22 <www.missiondata.io>

Jurisdiction	Data sharing initiative	General approach	Privacy measures	Implementation
L. European Union – Data Strategy	The EU announced the European Data Strategy[23] on 19 February 2020. This strategy aims to establish a European single market for data, and to build European data spaces for specific sectors, including energy data.	The Strategy is built on four pillars: ▪ an enabling legislative framework for the governance of common European data spaces; ▪ investments in data and infrastructures for hosting, processing and using data; ▪ empowering citizens to exercise their data rights; and ▪ establishing common European data spaces in strategic sectors and domains of public interest.	The Strategy states that: *European rules and values, in particular personal data protection, consumer protection legislation and competition law, must be fully respected.* It is expected that the proposed Data Act will include several new sections on the balance between privacy and access, including: ▪ facilitating decisions on which data can be used, how and by whom for scientific research purposes in a manner compliant with the GDPR; ▪ making it easier for individuals to allow the use of the data they generate for the public good, if they wish to do so ('data altruism'), in compliance with the GDPR; and ▪ making access to data compulsory (where necessary) under fair, transparent, reasonable, proportionate and/or non-discriminatory conditions.	The Data Strategy is new (February 2020) but it includes an ambitious timetable for implementation. For example, the legislative framework is to be in place by the fourth quarter of 2020, followed by a proposed Data Act in 2021. A key part of the Strategy is the establishment of data spaces. The two most relevant proposed data spaces are: ▪ an **Energy Data Space** to promote a stronger availability and cross sector sharing of data, in a customer centric, secure and trustworthy manner, to facilitate innovative solutions and support the de-carbonisation of the energy system; and ▪ a **Green Deal Data Space**, to use the major potential of data in support of the Green Deal priority actions on climate change and related issues.

[23] <ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en> and <ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf>

D. Lessons from data regulation in other sectors and internationally

1 A broad spectrum

The examples of local and international data sharing initiatives in Part C sit on a broad spectrum.

- **At one end, the initiatives are voluntary and light touch, with high level guidance and a distributed approach to implementation** (eg the telecommunications sector in Australia and the data sharing initiatives in Singapore and the USA). These initiatives are designed to aid market driven innovation. In practice, they have delivered some surprisingly positive results, including the development of a broad suite of innovative data products and even examples of consumer-initiated data sharing.

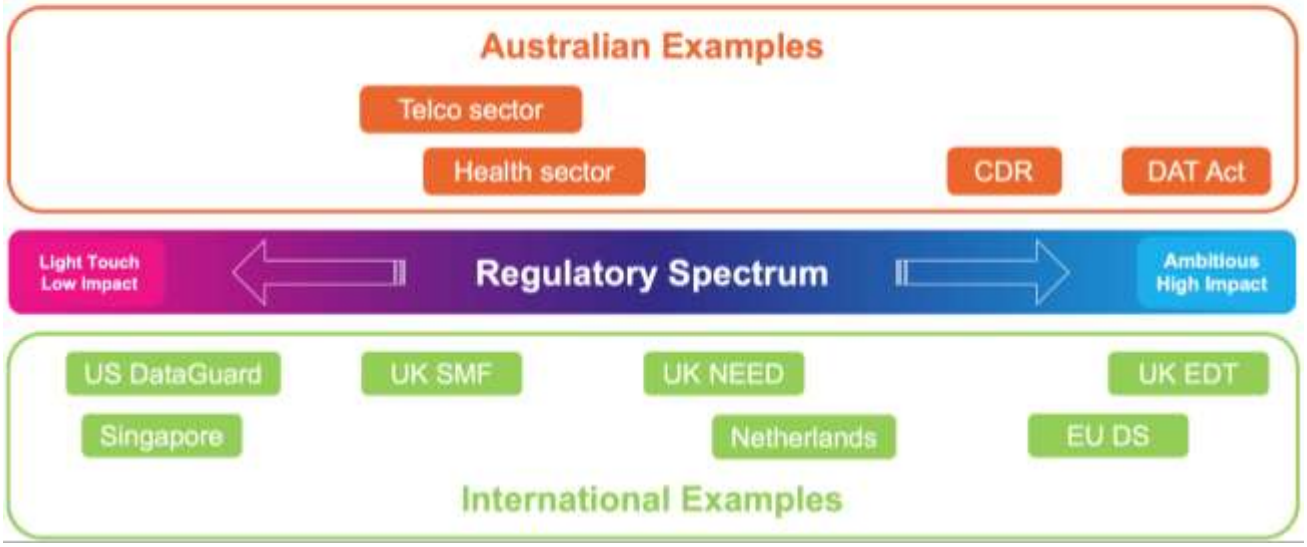
  However, these light touch initiatives appear to work best where there are very few privacy, confidentiality and secrecy barriers in place. For example, the US has very light touch privacy legislation. These approaches are unlikely to deliver significant outcomes in the energy sector in Australia, where a range of complex privacy, secrecy and confidentiality restrictions are in place.

- **At the other end of the spectrum are more radical and 'hands on' data sharing initiatives driven by new regulations that are deliberately trying to overcome barriers** (eg the proposed Energy Data Taskforce strategy in the UK and the Data Availability and Transparency Act (forthcoming) in Australia – and to a degree the CDR initiative in Australia). These initiatives attempt to 'switch' the default setting for data sharing from closed to open by introducing a presumption or a right that data can be shared, despite existing barriers, subject to conditions. This approach is relatively untested, but it appears to be the fastest route to enabling data sharing in environments where a range of complex barriers are in place.
- **In the middle of the spectrum are data sharing initiatives that try to overcome barriers to data sharing on a case-by-case basis, using a range of tools.** These include minor legislative reform, utilising exemptions and permissions in existing legislation, developing new data sharing agreements or contracts, and developing standards or guidelines. The initiatives are complemented by practical tools such as data hubs and data coalitions, so that the complexity of the 'behind the scenes' arrangements is hidden from most users. Examples include the Netherlands Energy Data Hub, the UK NEED initiative, and initiatives for sharing data in the health sector in Australia. The initiatives in this middle part of the spectrum are mature and have a good track record of providing some access to data, although they appear to require significant resources and are slow to develop. They share some similarities with the current situation in the energy sector in Australia, including many of the difficulties and barriers described in Part B of this report.

Local and international data sharing frameworks

Overview

- Broad spectrum of approaches to facilitating data sharing – both inside and outside the energy sector
- Some best practice is gradually emerging…



2 Key lessons from case studies

Table 7. Case study lessons

	Lesson	Examples
1.	There are advantages in switching to a presumption that all energy data can be shared, putting the onus on data holders to justify restrictions, rather than placing the onus on access seekers.	▪ A. Australia – CDR – Consumer Data Right ▪ B. Australia – DAT – Data Availability and Transparency Act (forthcoming) ▪ J. UK – Energy Data Taskforce
2.	There are advantages in managing privacy concerns through **conditions** for use of shared data rather than **restrictions** on access to data.	▪ A. Australia – CDR – Consumer Data Right ▪ B. Australia – DAT – Data Availability and Transparency Act (forthcoming) ▪ G. Singapore – Trusted Data Sharing Framework ▪ J. UK – Energy Data Taskforce ▪ K. USA – DataGuard Code ▪ L. European Union – Data Strategy
3.	Two clear models for implementing **user access to data** have emerged:	
	▪ **Membership** model – may raise complex competition and intellectual property issues.	▪ D. Australia – Telecommunications ▪ E. Netherlands – Data hub ▪ K. USA – DataGuard Code
	▪ **Accreditation** model – has resource implications, but it may be possible to leverage off the proposed accreditation models in DAT and CDR without having to start from scratch.	▪ A. Australia – CDR – Consumer Data Right ▪ B. Australia – DAT – Data Availability and Transparency Act (forthcoming) ▪ H. UK – NEED ▪ I. UK – Smart Metering Framework
4.	Two clear models for **acquiring data** have emerged. It may be possible to utilise aspects of both models for energy data in Australia.	
	▪ **Centralised** data hub / data catalogue model.	▪ A. Australia – CDR – Consumer Data Right – Energy ▪ E. Netherlands – Data hub ▪ H. UK – NEED ▪ I. UK – Smart Metering Framework

	▪ **Distributed** technology driven model, based on innovative technologies, for example APIs, blockchain, AI.	▪ A. Australia – CDR – Consumer Data Right – Open banking ▪ G. Singapore – Trusted Data Sharing Framework ▪ K. USA – DataGuard Code

3 Best practice approaches and common conditions on the use of shared data

Some best practice is emerging for the rules and conditions that should be applied to data sharing activities, in order to strike a balance between protecting privacy and facilitating use of data for a public benefit:

Table 8. Best Practice Approaches

Best Practice Approach	Examples
1. Providing a list of permitted purposes for use	▪ B. Australia – DAT – Data Availability and Transparency Act (forthcoming) ▪ C. Australia – Health ▪ H. UK – NEED ▪ I. UK – Smart Metering Framework
2. Providing a list of prohibited purposes for use	▪ A. Australia – CDR – Consumer Data Right ▪ B. Australia – DAT – Data Accessibility and Transparency Bill 2020 (forthcoming) ▪ C. Australia – Health
3. Applying a robust set of principles for privacy and security – with a consensus forming around the use of the Five Safes framework 1) Safe **People** – approved / accredited researchers 2) Safe **Projects** – all projects approved by an oversight body 3) Safe **Settings** – identifiable or sensitive data restricted to secure environments 4) Safe **Data** – where data is de-sensitised to the extent appropriate for the relevant People/Project/Settings 5) Safe **Outputs** – results checked for compliance with approved disclosure protocols[24]	▪ B. Australia – DAT – Data Availability and Transparency Act (forthcoming) ▪ H. UK – NEED ▪ J. UK – Energy Data Taskforce
4. Requiring vetted or accredited access to data	▪ A. Australia – CDR – Consumer Data Right ▪ B. Australia – DAT – Data Availability and Transparency Act (forthcoming) ▪ H. UK – NEED

[24] The 5 Safes framework is already being used to enable data sharing projects in the energy sector overseas. For an overview refer to: UK Data Service, *Legal and ethical challenges surrounding big data: energy data* (2020) <https://www.ukdataservice.ac.uk/media/604999/ukds-case-studies-ethical.pdf>.

		▪ J. UK – Energy Data Taskforce (limited to registration)
5.	**Restricting onward disclosure**	▪ B. Australia – DAT – Data Availability and Transparency Act (forthcoming) ▪ H. UK – NEED ▪ K. USA – Code
6.	**Managing de-identification and the risk of re-identification**	▪ B. Australia – DAT – Data Availability and Transparency Act (forthcoming) ▪ H. UK – NEED ▪ J. UK – Energy Data Taskforce

E. Reform Pathway

In this section we propose a non-linear, 3-step reform pathway, as outlined in the table below. Before considering these steps, we explore the implications of maintaining the status quo – that is, the high level impacts if none of the recommendations in this report were adopted.

#	Reform step	Summary
1	**Non-legislative improvements**	A reform package that uses non-legislative mechanisms to address some of the key issues with data collection and sharing
2	**Legislative improvements**	A legislative reform package that addresses some of regulatory barriers, without departing from the overall structure of the current regime
3	**Overhaul**	Fundamental principle changes to the existing confidential information and public interest data sharing regimes to create a new, fit for purpose public benefit data sharing regime

1 Status quo

In the future, without changes to the way in which data may be shared within the energy industry, we expect that the "status quo" will continue. We anticipate that a lack of coordinated action may inhibit innovation, worsen existing inefficient data management processes and prevent the ESB from achieving its goal of effective data management in the NEM. The concerns identified in Part B of our report, particularly in relation to privacy and confidentiality, are likely to continue.

For the ESB, this is likely to inhibit any progress towards the achievement of its desired outcomes from the Data Strategy, resulting in:

- delays and complex arrangements restricting Core Bodies from being able to share priority datasets with each other in a protected environment;
- limited rights and long negotiations affecting Core Bodies' rights to share priority datasets with Trusted Bodies in a protected environment;
- complicated and onerous public interest disclosure rights, which disincentivise sharing of priority datasets with Trusted Bodies and research institutions; and
- continued duplication of data collection and associated costs, without a single source of truth for each dataset and only partial visibility of existing datasets depending on the resources of the Core Bodies.

For the Core Bodies and the energy industry more broadly, this means:

- the presumption against sharing data will continue and the lack of sharing will come at a greater cost as the importance of data increases;
- data collection and use powers will remain fragmented, with the possibility of complex interactions and inconsistencies between the law and the rules;

- sharing of data will continue to be limited by conflicting interpretations and misaligned incentives and risks between data holders and data seekers;
- the lack of a clear framework that addresses and protects privacy, confidentiality and security appropriately will limit data disclosure as this may lead data holders to take ad hoc and inconsistent steps to manage the protection of the privacy interests of individuals and to avoid breaching obligations of confidentiality;
- even where data is shared, it is likely to be shared in a form or subject to conditions that limit the utility of the data for the desired public benefit purpose; and
- limits on transparency may lead to less accurate forecasting and planning, with the risk of repeating problems seen to date such as inefficient investment, higher consumer prices and impediments to technological development.

Examples of some of the issues that have arisen because under the status quo are set out below.

Example 1:

The ACCC has recently played a stronger role in the energy sector, including undertaking its Retail Electricity Pricing Inquiry and the related longer-term inquiry. An advantage for the ACCC in undertaking this work is its ability to compulsorily acquire data from market participants, including customer billing data from retailers, using its information gathering powers under section 95ZK of the CCA. Customer billing data is valuable in the energy sector for a range of policy reasons, including retail price monitoring and related reporting and statutory functions, but is largely unavailable as energy market bodies do not currently have the ability to obtain it from retailers. However, the ACCC operates under strict confidentiality requirements if information is collected under section 95ZK of the CCA. The ACCC has been constrained in its ability to share data with the energy market bodies and processes seeking to resolve this can take considerable time. The ACCC and AEMC explored the process requirements for data sharing in relation to customer billing data, but ultimately data sharing was not feasible.

Example 2:

AEMO and CSIRO sought a bilateral agreement for data sharing to allow CSIRO to provide support for NEAR. The complexity of negotiations caused substantial delay (more than 18 months) during a fixed funding window, reducing the potential benefits of NEAR funding. Privacy concerns have ultimately meant that metering data shared with CSIRO (through a protected environment) had to be de-identified to an extent which prevents linking to related research data. While this outcome will still provide significant insights that were previously not available to energy market bodies, the limitations have reduced the potential value of the data and limited the public-good analysis CSIRO can undertake. CSIRO's role in NEAR was intended to be to provide resourcing and skills to link and add value to key data sets to enable analysis previously not possible. However, now, any linking must be undertaken by AEMO, which has limited resources and competing priorities. As a result, the range of potential analysis has been constrained. Many linked data sets will also need to be aggregated to prevent re-identification, losing much of their potential benefit. These restrictions are required even though the data is being shared in a secure environment among trusted parties. For example, work is currently underway to link commercial building data with metering data to evaluate the impact of building policy and trends on commercial energy use, to improve demand forecasting.

Example 3:

ACCC, AEMC, AER, CSIRO, ECA, ABS, DISER and various state government bodies each undertake separate primary surveys of consumers in relation to energy bills and drivers of energy usage. The surveys are similar, but inconsistent. There are difficulties in sharing datasets between energy market bodies due to different ethical restrictions on how the information is collected and the way it can be used or shared. Many of these surveys also gained consent from consumers to link their responses to their meter data to better analyse impacts. However, inconsistent interpretations of regulatory requirements and fragmented data holders have made linking this data costly and difficult. The impact of this has been a duplication of time and resourcing for public data initiatives.

2 Improvements on the status quo

The first step on the reform pathway proposed is to address some of the issues with data collection and sharing in the energy regime identified above, without departing from the overall structure of that regime. This section 2 of Part E contains a series of non-legislative and legislative options to enhance data collection and sharing (each called "Improvements") while maintaining the essential elements of the existing regime (being a general prohibition on the disclosure of confidential and protected information with a series of exceptions for authorised disclosure).

Unlike the "Overhaul" option in section 3 of this Part E, the Improvements do not create a single, overarching framework that applies to all energy-related data held by Core Bodies and Trusted Bodies. The Improvements are, nevertheless, informed by emerging best-practice in data governance internationally to the extent possible. We have proposed flexible options to allow for changing data needs and technologies where possible. However, there are limitations on the extent this can be achieved within the confines of the current regime.

The Improvement options do not contemplate amending Commonwealth legislation so no improvements to the disclosure rights of the ACCC under the CCA are proposed in this section.

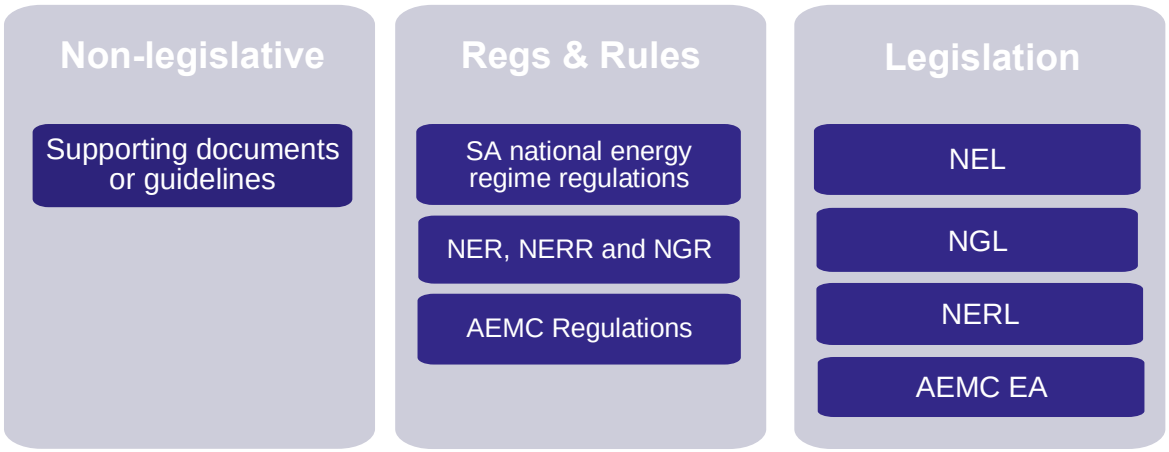
We note that the AER was given the right to disclose data to certain Commonwealth bodies under the "big stick" legislation (Treasury Laws Amendment (Prohibiting Energy Market Misconduct) Act 2019). Specifically, if the AER is satisfied that the information sought will enable or assist a Commonwealth body (broadly defined) to perform or exercise any of its functions or powers, then disclosure of the information to the entity would be an authorised use and disclosure of the information.[25]

To be considered viable options, the Improvements must:

- constitute a meaningful step toward the achievement of the strategic outcomes (even if they do not fully achieve them); and
- taken individually or together, offer a reform package that is comparatively less costly and faster to implement than the Overhaul option, relative to the gains likely to be achieved.

The Improvement options discussed in this section 2 of Part E are contained at all levels of state-based law:

[25] *Competition and Consumer Act 2010* (Cth), section 44AAF(3A) (Confidentiality).



The complexity and length of time to implement the Improvement options increases from low, in the case of the "Non-legislative" Improvements above, to high, in the case of the "Legislation" – which requires laws being passed by the South Australian Parliament.

While the Improvements could work as a package of reforms, they are not interdependent or sequential. Therefore, they can be actioned in tandem with other reforms or as interim steps toward the Overhaul option.

If an entirely non-legislative reform option is preferred, the supporting documents and guidelines could be created alone, or as a first step. These options have the advantage of being easily amended and being flexible to changing needs.

2.1 Non-legislative supporting documents and guidelines

2.1.1 Consistent information policies

Section 7 of Part B discussed the fact that data provided to Core Bodies, whether by compulsion of law or voluntarily, is often accompanied by claims of confidentiality. The interaction between contractual, equitable or moral obligations of confidence and the energy laws that authorise (but do not mandate) disclosure is not always clear. To alleviate some of the difficulties posed by accepting conditions of confidence, Core Bodies could implement consistent information policies.

The information policies could deal with the collection of data that has been given voluntarily and by compulsion of law in different ways:

- for data provided voluntarily, information policies could require Core Bodies to limit or avoid, where possible, acceptance of data provided under conditions of confidentiality. This may encourage Core Bodies to:
  - inform stakeholders about other protections that apply to their information;
  - consider the implications of accepting data voluntarily has on data sharing;
  - identify 'data gaps' in their collection powers; and
  - reduce inefficiencies such as duplication of collection across the Core Bodies; and

- for data required to be provided by law, it is unlikely that contractual or equitable obligations would be owed (see Section 7 of Part B), so to make this clear to the parties involved, information policies could indicate Core Bodies' inability to accept conditions on data use and sharing in these instances.

Core Bodies' information policies could also clearly notify data providers that information (including personal information under the Privacy Act) provided to the Core Body may be used and shared, in accordance with the law, for the purposes of fulfilling that Core Body's statutory functions.

The ACCC and AER's Information Policy is an example of this kind of policy, containing statements such as:

- "*In general, the ACCC/AER will not accept conditions that seek to limit the use of information to a particular matter.*"
- "*If the ACCC/AER has obtained information in the course of one matter which is relevant to another matter, the ACCC/AER will, in general, use that information in the context of the other matter subject to any specific legal requirement to the contrary.*"
- "*… ACCC/ AER function may also substantially affect other parties (such as access seekers or competitors) and some disclosure of information may be necessary for open and transparent decision-making.*"

Reviewing the Core Bodies' information policies with a view to:

- providing for greater use and sharing; and
- making the policies consistent (where appropriate),

could be an important first step in shifting the mindset of industry and energy market bodies towards greater acceptance of public-sector data sharing.

2.1.2 Data Sharing Agreement

In section 6 of Part B, we made the general observation that the incentives for data disclosure are misaligned in the current regime – data holders are considered to bear a disproportionate level of the risk and costs of disclosure, while data seekers receive the benefit. This was primarily due to our analysis in relation to:

- limitations with the current energy data regime, including practical limitations such as inconsistent systems and the absence of cost-allocation principles; and
- risk and liability for data disclosure (particularly in relation to personal information) not being adequately dealt with in the current regime.

During consultation with the Core Bodies and DISER, we proposed the creation of a template Data Sharing Agreement (**Template DSA**) for disclosure between Core Bodies and Trusted Bodies or with non-government data seekers. For use of the Template DSA to become accepted and common practice, it should be created by an appropriately resourced, representative working group with a strong governance structure.

There is precedent for this idea in the DAT Act, which will mandate data sharing agreements for all data sharing. On 22 April 2020, the ONDC released a "legislation-agnostic" data sharing agreement for consultation. The ONDC's draft is more principled and high-level than we would propose under a Template DSA for the energy sector. This is because there is a "responsibility to share" instruction

under the DAT Act framework, which would not necessarily apply to data sharing between Core Bodies and Trusted Bodies in the energy sector, so there is utility in more detail being agreed from the outset.

For example, a Template DSA for energy data could contain optional clauses and definitions which can be tailored to specific data projects with minimal time and cost. The Template DSA could cover similar content to the ONDC's "legislation agnostic" data sharing agreement (such as the parties to the agreement, description of the data, purpose for data sharing and conditions on data use), as well as:

- the legal basis of sharing;
- any safeguards to protect the data and project outputs (secondary sharing);
- cost arrangements;
- parties' responsibilities and liability, and any sanctions that may be imposed if the terms and conditions of the agreement are not adhered to; and
- standard data formats.

We received feedback on this idea. We acknowledge the concerns raised about the practicality of a Template DSA and the ability to overcome statutory barriers by way of contract. A key issue discussed was the differences between the DAT Act and the present situation. It was considered that:

- entities under the DAT Act may share more commonality of structure, governance and purpose than Core Bodies and Trusted Bodies in the energy context;
- as a result, the initial mediation and agreement of a DSA template or templates may be complex and time-consuming; and
- enforcement may be an issue.

We recognise that the Template DSA may need to include a high level, principled agreement between the parties to be supplemented with more detailed schedules (templates for which could also be considered). This is particularly the case where the data disclosure contemplated is not once-off, but an ongoing, collaborative project where the parties anticipate creating and co-owning intellectual property.

Agreeing to a Template DSA may be complex. However, there may still be efficiency in undertaking this work once to save time and costs in the future at least in relation to data sharing between particular Core Bodies who are likely to engage in data sharing on an ongoing basis between them in relation to datasets. This may also represent an opportunity to capture agreed policy and to create consistency in the treatment of energy data between Core Bodies and Trusted Bodies going forward.

2.1.3 Data Rule Change Policies

Section 5 of Part B of this report described the complex interaction between the energy data regime at the level of the law, which is broad and principles-based, and the Rules, which can sometimes be prescriptive on this issue (see Issue 3). In lieu of an option like the Overhaul proposed below, which replaces the current law and the Rules as the avenue by which data is shared, improvements could be made to the way data-related Rules are created and amended going forward. This would, over time, serve to bring the Rules into line with the policy behind the ESB's Data Strategy, encouraging greater data disclosure where it is safe to do so.

AEMC Rule Change policies

This reform could be brought about by new or amended AEMC policies that require both the Rule Change proponent and the Rule Change process to deal with data concerns in a structured and transparent way. In the first instance, the AEMC's two published guidelines for Rule Change proponents:

- '*The rule change process: A guide for stakeholders*' (June 2017); and
- '*Applying the Energy Market Objectives*' (July 2019),

could be amended to request proponents to consider the data impact of a proposed Rule Change. Proponents could be requested to consider criteria to deliver on the principles that:

- data should be "open where possible, closed where necessary"; and
- sharing between Core Bodies should not be fettered.[26]

The AEMC could introduce an internal policy that requires consideration of the same principles and the implications of any data created by a Rule Change. This policy could deal with the mechanics of a data related Rule Change by requiring:

- a general preference for principles-based approaches to data-related rules where appropriate;
- consistent use of terminology in the Rules concerning data collection, use and disclosure;
- consistent cross-referencing to the NEL; and
- a formula of words to be used where disclosure is "authorised by law" or "required by law" in accordance with the Privacy Act.

MCE Statement of Policy Principles

It may be considered desirable to elevate the data-related Rule Change principles and policies mentioned above to convey their strategic significance. In this case, the ESB could consider requesting the MCE to issue a Statement of Policy Principles. Section 8 of the NEL provides that the MCE may issue a Statement of Policy Principles in relation to any matters relevant to the exercise and performance by the AEMC of its functions and power in making a Rule.

2.2 Regulatory amendments

2.2.1 Prescribe Trusted Bodies that AEMO and AEMC may disclose to

Core Bodies' current rights to share data with other Core Bodies and some Trusted Bodies is summarised in section 3 of Part B. Both AEMO and the AEMC have the right to share "protected information" and confidential information with (among others):

- each other;
- ACCC;
- AER;
- ESB; and

[26] These are only guides so AEMC could not *require* an applicant to do so without changes to regulations.

- any other person or body prescribed in the relevant regulations (currently none for AEMO).

AEMO and the AEMC may impose conditions on the above bodies in relation to the information shared under these rights.

The *National Electricity (South Australia) Regulations* (SA) and the *AEMC Establishment Regulations 2005* (SA) could be amended to prescribe "Trusted Bodies" that AEMO and the AEMC can share data with. The bodies could be prescribed in two classes, with different regimes applying to each:

- "**Class A**" prescribed bodies could include State governments, Commonwealth agencies and other Trusted Bodies; and
- "**Class B**" prescribed bodies could include any other bodies deemed to be appropriate, such as CSIRO, research institutes or universities.

This option may be more relevant to AEMO than to the AEMC, which faces fewer challenges sharing the data it controls.

Class A prescribed bodies

Class A prescribed bodies could be treated in much the same way as Core Bodies. That is, where Core Bodies share data with Class A prescribed bodies:

- the disclosure of personal information is permitted under the Privacy Act;
- confidentiality of the information is otherwise preserved; and
- most importantly, other principles relating to data security, such as considerations of the appropriate data format, environment, intended use or outputs, would not be required.

Of course, as described in section 6 of Part B above, some obligations under the Privacy Act continue to apply in respect of personal information which has been disclosed, such as the obligation in APP 11 to take reasonable steps to protect the security of personal information that it holds.

This treatment of Class A prescribed bodies is consistent with the principle gaining traction internationally that data is received and held by government entities as custodians, and that use of public data comes with a commensurate responsibility to act in the interest of the public. Where data is shared between government entities, those government entities also share responsibility for the data's protection and the stringent protections that would be required if data was being shared with private organisations or otherwise outside the remit of the government need not apply.

Consistent with these considerations, we suggest that imposing conditions on Class A prescribed bodies receiving data would not be appropriate.

Class B prescribed bodies

In the case of Class B prescribed bodies, however, additional security may be warranted, particularly when considering appropriate data projects and outputs of the data seeker (ie secondary disclosure). The obligation to satisfy the data holder that these protections are met could be placed squarely on the data seeker. Either the law, the regulations or policies could provide that, in order to receive data, "Class B" prescribed bodies must establish, to the reasonable satisfaction of the data holder, that the proposed use of the data is for an appropriate purpose and has an appropriate output, for example because:

- it is “reasonably necessary to inform a policy, program, service delivery or for research and developing that is in the long-term interest of consumers of energy” (in line with the proposed DAT Act); or
- it has reasonable prospects of delivering benefits that are in the long-term interests of consumers of energy; and
- it will not be disclosed or published in a manner that enables the identification of the people that provided the data originally.

We acknowledge that being satisfied of these matters is not an easy task for a Core Body like AEMO. As discussed in section 5 of Part B in relation to the public benefit sharing regime, determining what is in the long-term interest of consumers is challenging, particularly in the absence of a right to compel detailed information about the data seeker’s intended use of the data (see Issue 2 above). In the absence of greater guidance therefore, this reform may not result in significantly increased flows of data. In order to increase the flows of data, it may be necessary to hand the decision-making process to another entity (as canvassed in section 3.3.4 below), such as a data sharing panel of experts appointed for this purpose.

We note that a working group founded under the NEAR Program is currently developing NEL and NER changes to facilitate the sharing of data between AEMO and CSIRO for the purposes of that program. There should be consistency between the reforms proposed in this report and any amendments developed for the NEAR Program.

Another limitation of this Improvement option is that the list of Class B prescribed bodies is static and the regulations must be amended to change or add to it. On the other hand, it is relatively more flexible than changing the list of bodies currently prescribed in the law.

Further consideration will be required as to the legal means of imposing conditions on Class B prescribed bodies, for example, whether it can be done by regulations only or would require changes to the legislation.

2.2.2 Amend problematic Rules

In section 4 of Part B, we discussed AEMO’s broad rights under section 53D of the NEL and section 91FD of the NGL to use data it obtains in any way for any purpose related to its statutory functions. One issue AEMO faces in relying on these rights, as discussed above, is their potential to be “read down” by the level of prescription found in the Rules.

Rather than amending the law, one option is to amend the problematic rules. This can be done without the need for legislative amendment. Two clear examples of such Rules which consistently create issues are provided in the table below.

Rule	Description / extract	Issue
7.10.1(a)(7)	**Metering data and NMI standing data** "*Metering Data Providers must provide … the delivery of metering data and relevant NMI Standing Data to AEMO for settlements*"	▪ Imply that use by AEMO for any other purpose is prohibited. ▪ Suggest that disclosure of this data to Core Bodies under the NEL is prohibited, as those Core Bodies do not fulfil settlement functions.
7.11.1(f)	**Settlements ready data** *"The settlements ready data held in the metering database must be used by* AEMO *for settlements purposes*"	

2.3 Legislative amendments

2.3.1 Clarify AEMO's right to use of information

An alternative to amending the Rules to provide greater clarity is to amend the legislation to achieve a similar outcome as amending the Rules in section 2.2.2 immediately above.

To address this, the laws could be amended to reflect the policy intention that no restriction on AEMO's use of data is necessary or desirable. This would avoid AEMO ever having to consider whether a rule such as clause 7.11.1(f) of the NER, for example, is intended to restrict AEMO's broad data use right in the NEL/NGL.

This amendment may look something like:

53D—Use of information

(a) AEMO may use information obtained by market information instrument or in any other way for any purpose connected with the exercise of any of its statutory functions.

(b) Nothing in this Law, the Rules or the Regulations restricts the operation of paragraph (a).

This would require a consequential amendment section 52(2) and to the Note in that section.

We also considered a second option, which would provide that any abrogation of AEMO's broad use rights under section 53D of the NEL and section 91FD of the NGL in a rule or procedure must be done with express reference to those sections. This would avoid AEMO having to "take a view" as to whether clause 7.11.1(f), for example, is intended to restrict AEMO's broad data use right in the NEL/NGL. However, this option was not considered the preferred option, as there is not a sound policy reason to prevent AEMO using information that would assist it in the performance of its statutory functions.

2.3.2 Broaden the AEMC's right to disclose data (s24 AEMC EA)

As outlined in section 3 of Part B, the AER and AEMO have the right to release data to anyone in certain circumstances, without any further restriction, including:

- where consent has been obtained; and
- in de-identified or sufficiently aggregated form.

The AEMC does not have these rights. We consider that consistency in the disclosure rights between the Core Bodies is desirable to allow consistency of information policies, improve communication and make the introduction of other improvements simpler. To achieve this the AEMC EA could be amended to provide the AEMC with the authority to disclose confidential information to anyone with consent or where de-identified or sufficiently aggregated.

2.3.3 Broaden the AER's power to disclose data (s44AAF(2) CCA)

Just as the *National Electricity (South Australia) Regulations (SA)* and the *AEMC Establishment Regulations 2005* (SA) allow the prescription of additional bodies that AEMO and the AEMC can share data with, section 44AAF(2) of the CCA permits the AER to disclose confidential information to the extent required or permitted by state legislation. A similar approach could therefore be followed to that proposed in section 2.2.1 for the benefit of the AER, by amending the NEL, or another state law, to prescribe additional bodies (Class A or Class B) that the AER may disclose to.

2.3.4 Broaden the public benefit disclosure regimes (ss54 and 28ZB NEL and 91G and 329 NGL)

As discussed in section 3 of Part B, AEMO and the AER have rights to disclose data to anyone (whether selected individuals, selected entities or the public at large) where there is an overriding public interest in doing so. For the reasons listed in sections 5 to 8 of Part B, however, these public benefit disclosure regimes are not currently being used by AEMO and are only relied on by the AER for discreet disclosures of one-off data sets, where the individuals concerned are able to be consulted.[27]

In consultation with Core Bodies, we proposed options to make the public benefits disclosure regime more workable including:

- relaxing the overly onerous notice requirements (see section 5 of Part B, Risk 2);
- creating detailed policy guidelines to assist decision-makers to decide whether disclosure is in the public interest; and
- clarifying the applicability of Core Bodies' immunity for any impacts of disclosure.

The feedback we received at the workshop was that, even with these proposed amendments, the regimes would be of limited utility because:

- AEMO and the AER would retain the onus of satisfying themselves that the benefit of disclosure outweighs any potential detriment to persons to whom the data relates. This is not a simple task, even with guidelines to assist, because the output of the data seekers' use is generally unknown and is beyond the control of AEMO and the AER; and

[27] AER, Confidentiality Guideline, August 2017.

- there are relatively few discrete data sets that are appropriate for one-off release in this way. This regime is more difficult to apply to dynamic datasets, because the notice requirements and public benefit/detriment test would need to be done each time data was proposed to be released or a "standing" consent obtained.

As a result, we have formed the view that the public benefit disclosure regimes cannot be usefully improved in their current form and, if data disclosure to entities beyond the Core Bodies and Trusted Bodies captured in Class A and Class B prescribed bodies is desired, a more fulsome reform package should be considered. The Overhaul option discussed below proposes removing the public interest disclosure regimes in the law and replacing them entirely.

3 Overhaul

The third proposed option in the reform pathway is to "overhaul" the energy data framework to replace the existing public benefit disclosure regime referred to in section 5 of Part B with a new fit for purpose public benefit data sharing regime.

This option proposes some key concepts and principles that may be used to guide the development and design of this third option in a way that enables Core Bodies and Trusted Bodies to share clearly defined datasets for specified public benefit purposes with appropriate safeguards in respect of privacy, confidentiality and security.

3.1 Selecting the appropriate framework

We considered the following alternative approaches as the first step in designing a new data sharing framework:

1 **designing a bespoke regime** – a bespoke regime could be designed to achieve all the ESB's outcomes for its data strategy. However, the design process would require significant time, resources and effort to develop. More importantly, it could take significant time to educate and inform stakeholders and get them to accept and support a new data sharing paradigm, particularly without an existing frame of reference; and

2 **"leveraging" frameworks and design principles from an existing regime** – the concepts, structure and principles from existing data sharing frameworks could be adapted to apply to the energy sector. In this regard, we considered the advantages and disadvantages of adapting the two principal existing data sharing models in Australia:

- the CDR, by which consumer data is shared between trusted entities at the direction or authorisation of a consumer; and
- the DAT Act, by which data is proposed to be able to be shared between certain Commonwealth government agencies for a public benefit.

Approaches	Advantages	Disadvantages
Bespoke regime	▪ Can be tailored to achieve each of the ESB's outcomes ▪ Will be appropriate for the nature and specific requirements of energy data	▪ Significant time and resources to develop ▪ No existing public engagement ▪ Requires stakeholder and market education
Leverage CDR	▪ Robust data sharing regime ▪ Extensive public consultation and government support ▪ Amendments to legislation and associated rules have been enacted ▪ Includes detailed privacy safeguards and information security measures	▪ Data sharing requests are initiated by consumers (rather than energy market bodies) ▪ Does not apply to government entities ▪ May not be aligned with ESB's Data Strategy outcomes ▪ Not yet tested
Leverage DAT Act	▪ Robust data sharing regime ▪ Extensive community consultation and government support ▪ Data sharing model is easily applied to other sectors ▪ Aligned with ESB's Data Strategy outcomes ▪ ACCC, AER, CER and DISER will be familiar with the DAT Act and CSIRO might be accredited under the new regime	▪ Applies only to public sector data held by Commonwealth bodies (however all entities including State and Territory authorities and private sector entities can apply for accreditation and access) ▪ Draft legislation has not been released ▪ The pause on consultation on the Exposure Draft reduces the benefit of leveraging the DAT Act ▪ Not yet tested

Questions to consider:	
1.	**Are there other data sharing models or frameworks that should be considered?**
2.	**Based on the above analysis, is the DAT Act the best framework to adapt for data sharing in the energy sector?**

3.2 Legal mechanism

The next threshold question is what legal mechanism is required to implement a new data sharing regime. Ultimately there are three possible methods to effect the required change in legislation:

- **extend the DAT Act** to the energy sector, so that State and Territory agencies (such as the AEMC) and AEMO are part of, and subject to, the regime (see "Extend DAT Act" below);
- **create a new law** (whether that is a new cooperative State law, or a new Commonwealth law or new provisions in an existing Commonwealth law (such as the CCA)) to apply the DAT Act principles (with adaptations as appropriate) to the energy sector (see "New laws" below); or
- **amend the existing energy laws** to include the principles from the DAT Act (with adaptations as appropriate) (see "Amend existing laws" below).

However, there is additional legal complexity in implementing a new data sharing regime based in legislation that confers functions, rights and obligations upon both State authorities and entities, as well as Commonwealth entities. This complexity would need to be addressed and resolved in due course if this option was considered appropriate.

Methods	Advantages	Disadvantages
Extend DAT Act	▪ Legislative framework for data sharing between government agencies has been prepared but has not been released for consultation	▪ Exposure draft of DAT Act not released ▪ May not be appropriate to have Commonwealth law regulating State-based regimes ▪ May not be appropriate for the energy sector or the objectives of the ESB Data Strategy
New laws	▪ Can be tailored from the ground up to achieve each of that ESB Data Strategy objectives	▪ Complexity in the adoption of cooperative State-based laws ▪ May not be appropriate to have Commonwealth law regulating State authorities and entities ▪ May be difficult to have State-based regimes conferring functions on Commonwealth entities ▪ Could create an additional layer of legislation which increase complexity
Amend existing laws	▪ Maintains existing energy law framework and reduces legislative complexity ▪ Amending existing energy laws is a process that is familiar for	▪ Additional complexity in dealing with the existing data use and sharing rights in a way which does not produce inconsistencies

	stakeholders and market participants	▪ May be difficult to have State-based regimes conferring functions on Commonwealth entities

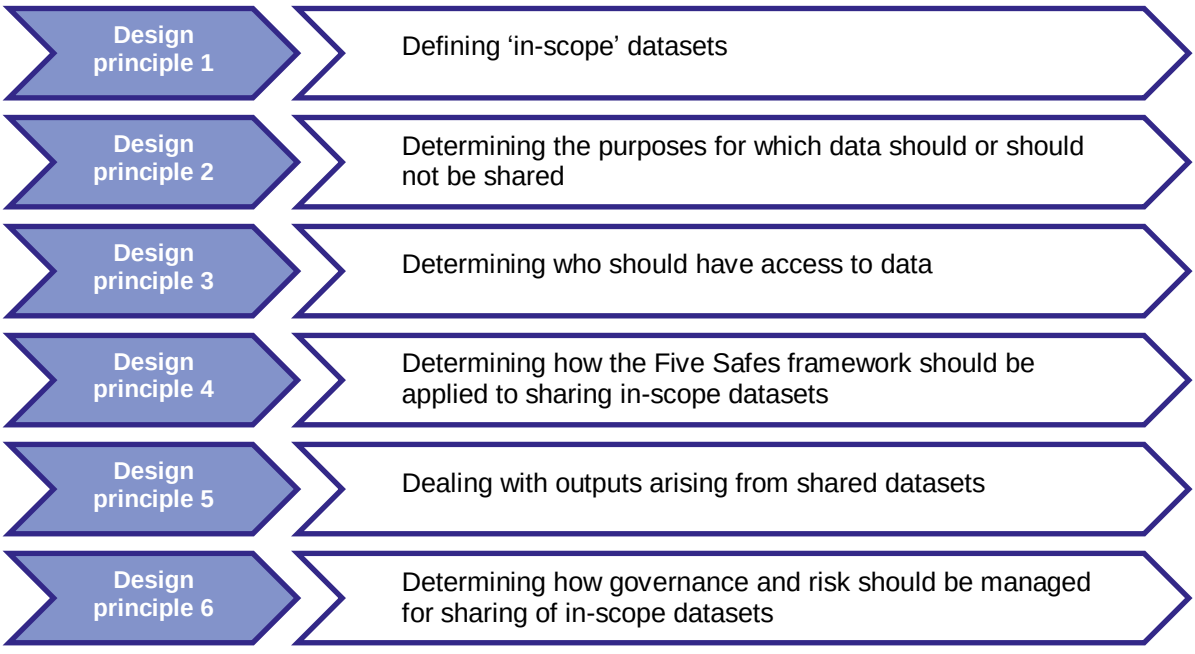
Questions to consider:	
1.	**Which is the preferred option for implementation of a new data sharing regime?**
2.	**Should the ESB consider implementing changes proposed in option 2 (Improvements) while working through the details in option 3 (Overhaul)?**

3.3 Design principles

Assuming for the purposes of this report that leveraging and appropriately adapting the DAT Act principles is preferred (despite the pause in consultation on the Exposure Draft of the DAT Act), we have used a combination of the Department of Prime Minister and Cabinet's:

- Data Sharing and Release Discussion Paper
- Best Practice Guide to Applying Data Sharing Principles
- New Australian Government Data Sharing and Release legislation Issues Paper for Consultation

to derive a number of design principles that will need to be considered in order to develop an energy data sharing regime applicable to energy that will act to meet the objectives of the ESB Data Strategy.



Relevant considerations for each of the design principles are set out below, including additional policy questions which will need to be considered in order to progress the development of the model.

Questions to consider:	
1.	**Are there any other design principles that should be considered?**

3.3.1 Design principle 1 – defining 'in-scope' datasets

A well-designed energy data sharing regime will define datasets in a way that:

- enables participants in the regime to clearly identify in-scope and out-of-scope datasets; and
- facilitates the inclusion of new in-scope datasets and new out-of-scope datasets as and when required to ensure the regime can adapt and respond to changing data needs within the energy sector.

We have set out in **Appendix 5** a worked example of the process for determining whether a dataset falls within the definition of AEMO's 'Protected Information' under the current energy law framework which illustrates some of the problems that can arise without a clear means of defining datasets. It is apparent from this that the current way in which datasets are defined under the current energy law framework:

- utilises a confusing mix of both principled, technical and prescriptive definitions;
- cuts across the legislation, Regulations, Rules and Procedures (but the prescriptive definition in the Rules and Procedures does not logically interact with the principled definition set out in the legislation);
- contains overlapping definitions relating to categories of data, meaning one dataset can fit within multiple definitions; and
- contains inconsistent terminology when referring to key energy datasets, which results in difficulties in interpreting rights and obligations in relation to data sharing.

Considering this design principle, we suggest a mix of both principled and prescriptive definitions be used to define in-scope and out-of-scope datasets. We set out further details below to illustrate how such a mix could work.

New legislation should set out a definition with:

- an overarching **principled element** such as "*datasets collected or created by a Core Body or Trusted Body in connection with or for the purposes of performing that entity's statutory functions or powers in relation to [X]*";[28]
- a process for identification or specification of datasets that are **excluded** from the scope of the operation of the regime; and
- a **prescriptive non-exhaustive element** that will incorporate a new 'Dataset Glossary' in a separate document that clearly sets out:

[28] This is intended to allow for the inclusion of limitations that restrict the broad scope of the principled element, particularly for agencies or organisations with a broad set of functions where only some of which relate to energy.

- the name and description of specific energy datasets within the principled element which are predetermined to be in-scope of the regime;
- technical specifics relating to each dataset (including location, security environment and quality); and
- the data holder for each dataset.

In addition to the specific datasets that are excluded from the scope of the operation of the regime, any datasets that are not listed in the Dataset Glossary would be considered out-of-scope for the purposes of data sharing.

It is intended that the NER, NGR and NERR would provide for the creation of the Dataset Glossary and set out the mechanism by which datasets can be included in, or removed from, the list of in-scope and out-of-scope datasets. The Dataset Glossary is intended to ensure:

- clarity through standardised and consistent terminology. This will assist to ensure all participants in any data sharing arrangements under the energy data sharing regime will be using shared terminology that will act to assist in ensuring all participants are 'on the same page'; and
- flexibility as it will be a 'living' document separate from the Rules or legislation that can be updated as and when required to adapt and respond to changing data needs.

There would also be an opportunity to review the current definitions relating to data categories in the existing Rules and to update and amend such definitions to utilise the consistent terminology set out in the Dataset Glossary. This would ensure the benefits of this reform are seen beyond just data sharing among public energy bodies but across the energy sector more broadly.

Questions to consider:	
1.	**How should in-scope or out-of-scope datasets be defined?**
2.	**What incentives should be built into the regime to encourage energy market bodies to include more (rather than less) datasets in the sharing regime?**
3.	**What processes and governance should apply to the addition or removal of in-scope datasets?**
4.	**What are the consequences of removing an in-scope dataset for pre-existing users of those datasets?**

3.3.2 Design principle 2 – determining the purposes for which data should or should not be shared

A key requirement of the DAT Act is that all data sharing must meet a high level 'purpose' test.

- To satisfy the current purpose test in the DAT Bill, sharing data must "*be reasonably necessary to inform government policy, programs, or service delivery, or be in support of research and*

development".[29] *In addition, data sharing for any other purposes, including for "compliance and assurance activities and national security and/or law enforcement*",[30] is not permitted.

Like the DAT Act, we propose that data shared under the energy data sharing regime will need to satisfy a bespoke purpose test.[31] The development of the purpose test will involve weighing up the public benefits of sharing energy data with legal and ethical considerations such as legal rights and interests relating to privacy and confidential information.

Getting the purpose test right is fundamental for engendering trust in the energy data sharing regime as well as ensuring data can be utilised in was that achieve the objectives of the ESB Data Strategy. As such it is important that broad public consultation is undertaken when determining the purposes for which data should or should not be shared.

We suggest the following as a starting point for consultation and discussion:

Permitted data sharing	Prohibited data sharing
▪ Based on DAT Act*: reasonably necessary to inform [government] policy, program [and service delivery], or for research and development.* This is based on permitted purpose from the DAT Act, however it should be considered whether such a test would be appropriate for the aims of the ESB Data Strategy which focuses less on program and service delivery and more on energy specific objectives such as those set out below. ▪ Based on ESB Data Strategy: *reasonably necessary to inform operation and development of the energy market, wider government policy and services, or for research and development in the energy sector.* This formulation is based on the aims of the ESB Data Strategy and maybe more appropriate for an energy specific data sharing regime. ▪ Based on National Energy Objectives: *beneficial for the long-term interest of consumers in the energy sector*. There may also be other formulations to consider and we suggest consulting broadly on this issue as it will form a key part of the regime.	▪ Based on DAT Act: *data sharing for assurance (including eligibility, entitlement or liability) and compliance*. We note that while use of data for these purposes has been carved out of the DAT Act, in the context of the energy sector, it would be important to consider the appropriateness of importing a similar prohibition in light of the AER's and the ACCC's compliance and assurance functions and whether such a prohibition could undermine some of the purposes for which relevant energy agencies would need to share data and the potential benefits of a revised data sharing regime in energy.

Questions to consider:

[29] PM&C, Data Sharing and Release Legislative Reforms, Discussion Paper (September 2019), Page 17 and 21.

[30] PM&C, Data Sharing and Release Legislative Reforms, Discussion Paper (September 2019), Page 25.

[31] It has become common to include a purpose test or a set of permitted purposes in legislation addressing data sharing. Recent examples include: *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth); *My Health Records Act 2012* (Cth); and *Health Legislation Amendment (Data-matching and Other Matters) Act 2019* (Cth).

1.	**How should "purposes" be defined?**
2.	**What purposes should be prohibited in the context of the energy sector?**
3.	**How much flexibility is needed to expand or narrow these purposes in the future?**

3.3.3 Design principle 3 – determining who should have access to data

Under the DAT Act the ability to be accredited and apply for data access (including commercial entities) is not restricted. However, the applicability of this approach should be considered in the context of the energy sector as it may be more appropriate for a data regime in energy to be designed, from the outset, to limit data sharing to certain defined and authorised energy market bodies.

Relevant considerations for the energy sector might include:

- access to data should initially be limited to specific entities where it is clear that the data will be used for a public benefit. This would include the Core Bodies in Group 1 below;
- access to data beyond the Core Bodies (Group 2 entities below) should be given via a clearly defined authorisation or accreditation which is both flexible and revocable;
- whether or not the concept of reciprocity should form part of the regime (as is the case in the CDR);
- access could be scaled (ie authorised access seekers can be categorised into conceptual groups, each with different or tiered rights and obligations in respect of different datasets); and
- how should the accreditation regime be implemented and monitored and what governing body should be responsible for decision making and enforcement in relation to accreditation.

When considering these principles in the context of the energy sector, three groups should be considered separately:

A phased approach could be considered for Groups 1 and 2.

This report does not include Group 3 members in the data sharing regime for a number of reasons:

- consumer data sharing is the subject of the CDR in energy, and so does not need to be dealt with in this data sharing regime; and

- giving private sector entities (such as market participants and new energy service providers) access to datasets collected by public bodies raises significant issues that are beyond the scope of this report. These include use of information in those datasets for marketing purposes or for other privacy intrusive purposes, as well as the increased risk of data breaches that arises when information is widely held by entities in the market.

Questions to consider:	
1.	**Is the categorisation into the three groups above appropriate?**
2.	**What process should apply to adding new organisations into Groups 1 and 2?**
3.	**Is authorisation or accreditation required to add new organisations into Groups 1 and 2?**
4.	**What kinds of processes should apply to the removal of entities from Groups 1 and 2 or removal of their authorisation or accreditation?**
5.	**Is it appropriate for Group 3 entities to be part of the sharing regime?**

3.3.4 Design principle 4 – determining how the Five Safes framework should be applied to sharing in-scope datasets

The ONDC developed the 'Data Sharing Principles' (**DSPs**) as the risk management framework for sharing under the DAT Bill. The DSPs are based on the Five Safes framework, but strengthen privacy safeguards, among other things.[32] They will be a core component of the framework to be established under the proposed DAT Act.

The Five Safes framework is a framework which is internationally recognised and applied to govern the conditions on which data can be safely shared, and how risks of data sharing can be minimised and mitigated by determining the specific controls to be applied for each data sharing activity. We set out below how the Five Safes framework may work in the context of energy data sharing using an example from the UK energy sector:

[32] <https://www.datacommissioner.gov.au/safeguards/sharing-principles>

The 5 Safes framework is already being used to enable data sharing projects in the energy sector overseas.

UK energy sector conducts some research projects using the 5 Safes

- Combines household energy consumption data and smart meter data with other sources:
  - Household Survey demographic data
  - Environmental Performance Certificates
- Impressive research outputs to date:
  - Government outputs on energy poverty
  - Industry outputs re consumption peaks

Regulatory framework:

- UK guiding principle is that "**data is open where possible and closed when necessary**"
- Use the consent provisions in the *Data Access and Privacy Framework* set out in the *Smart Energy Code* for access to smart meter data
- Use the *5 Safes Framework* for access to other data sets and managing outputs

Five Safes	Principle	Implementation (UK)
Safe People	• Can the third parties we are providing the data to be trusted to use it in an appropriate manner?	• Researchers must be approved / accredited • (Note: the accreditation process is being updated in the UK as part of the Energy Data Taskforce recommendations)
Safe Projects	• Is the use of the data appropriate?	• All projects must be approved by a Data Access Governance Board
Safe Settings	• Does the environment in which the data is shared minimise the risk of unauthorised use or disclosure?	• Identifiable or sensitive data will reside in approved Secure Lab environments where analysis will be conducted
Safe Data	• Are appropriate and proportionate protections applied to the data? • (Note: the Safe Data Principle focusses on what treatment of the data (data minimisation, aggregation, removing direct identifiers or suppressing individual records) is necessary).	• Where possible data will be de-identified before release to researchers. Identifiable data can only be analysed in secure environments
Safe Outputs	• Can the results of the project be published without identifying the people that provided the data originally?	• Results must comply with Statistical Disclosure Control protocols and will be checked before they can be published

Beyond the principles of the Five Safes, it is also worth considering the mechanics of how the Five Safes framework / DSPs applies under the DAT Act:

- the DSPs have also been designed to be applied jointly and iteratively by both the data custodian and the user seeking it;

- if agreement on the application of the DSPs **cannot** be reached, data cannot be shared. The DAT Act will not provide for merits review of a data sharing decision made by the data holders (although other avenues for review may exist);
- if agreement on the application of the DSPs **can** be reached, the details of the DSP assessment will then form part of a Data Sharing Agreement (DSA). The DSA will be on standard terms and will include details as to how the data sharing meets the purpose test and other safeguards that ensure the purpose is authorised;
- all DSAs will be published on a public register for greater transparency; and
- the ONDC will update the *Best Practice Guide to Applying the Data Sharing Principles* and will produce more guidance on the Data Sharing Principles as needed.

In applying the Five Safes / DSPs framework to energy data sharing, there may be merit in considering the following alternative mechanisms:

Potential alternative positions to the DAT Act	
The data seeker (rather than the data holder) could be made responsible for undertaking the initial Five Safes assessment for approval by the data holder.	It could be more appropriate for the data seeker to be responsible for resourcing and carrying out the initial Five Safes assessment, which would need to be approved by the data holder. While the data holder does have a greater understanding of the nature of the data, arguably, the data seeker has greater responsibility and control over safeguards relating to limited use within the permitted purpose and ensuring it has the appropriate security environment required for the dataset. Imposing this task on the data seeker instead of on the data holder: ▪ would mitigate resourcing and priority concerns for data holders; ▪ potentially result in efficiencies; ▪ aligns responsibility for security with the benefit of obtaining the data; and ▪ would not change the requirement for the data holder to be satisfied that the Five Safes assessment is adequate.
A dispute resolution process or independent expert determination process is available to data seekers whose requests have been rejected	Rejecting a data sharing request under the Five Safes framework should not be a common occurrence. The Five Safes is intended to provide for mitigation measures and safeguards that would minimise risk rather than prevent the sharing of data all together. However, we acknowledge that data holders and data seekers often have different interests and risk profiles which could lead to disagreement even within the Five Safe framework. Providing data seekers access to independent experts or other such dispute resolution mechanisms may ensure objectivity in relation to contentious data sharing projects.

	Data holders would still retain their good faith immunity regardless of the outcome of any dispute process or independent review. We note however that the DAT Act is not expected to permit data seekers to access any mechanism for ONDC review of decisions by data holder (for example, decisions in relation to whether data will be shared and conditions on sharing) on the assumption that the data holder is best placed to determine the risks and benefits of sharing.

Questions to consider:	
1.	**How can we best incentivise data sharing while balancing inherent risks?**
2.	**If the Five Safes assessment is undertaken by the data holder, how can we incentivise that to be done in an efficient and timely manner and in a way that facilitates data sharing rather than discouraging data sharing?**
3.	**Should the responsibility for conducting the Five Safes assessment rest with the data seeker or the data holder?**
4.	**Should there be a charge payable to the data holder to compensate it for the cost of reviewing a request for data access?**
5.	**What happens if a data holder does not approve a Five Safes assessment undertaken by a data seeker?**
6.	**Should there be a defence from liability for a data holder who releases a dataset if it is satisfied with a Five Safes assessment?**

3.3.5 Design principle 5 – dealing with outputs arising from shared datasets

Under the data sharing arrangement facilitated by the DAT Act we expect that practically, outputs arising from the use of shared datasets could be managed in two ways:

- the Data Sharing Principles will act as a framework to manage the risk of 'on-disclosure' via outputs to the extent that they might require, or reveal access to, underlying datasets; and
- standard DSAs may be used to govern how the intellectual property in outputs relating to shared datasets will be owned or licenced.

In our view, in the energy sector the ownership of intellectual property in outputs and the ability to publish those outputs will be an important issue in considering whether or not to extend the energy data sharing regime to accredited research institutions in Group 2 (noting there is no proposal regarding 'grouping' in the proposed DAT Act – this will be a specific customisation for the energy sector). More work will need to be done to identify the kinds of licensing models which might be acceptable to both Core Bodies and Trusted Bodies, as well as to accredited research institutions.

Questions to consider:	
1.	**What regime should govern intellectual property outputs arising out of research and development activities?**
2.	**Should data-sharing parties be able to obtain commercial value from the intellectual property generated from the use of shared energy data?**
3.	**Should outputs be able to be used for commercial uses and do those commercial uses need to be in the public interest?**
4.	**Should accredited research institutions be subject to a condition of access to data that any outputs must be released as "open data" or under a creative commons licence?**
5.	**How should use and compliance be monitored?**

3.3.6 Design principle 6 – determining how governance and risk should be managed for sharing of in-scope datasets

Governance

Under the DAT Act, we understand that the National Data Commissioner will have a responsibility to regulate the data sharing in a manner that promotes trust, taking a graduated enforcement approach and applying proportional responses to deter future non-compliance. The regulatory functions of the National Data Commissioner are likely to include:

- accrediting users and data service providers, and facilitating an internal review of accreditation decisions (external review will be via the Administrative Appeals Tribunal (**AAT**) and the courts where appropriate);
- handling complaints from participants in the scheme;
- monitoring compliance with the legislation, including conducting assessments and investigations; and
- determining breaches of the legislation.

There will need to be a similar governance structure for a data sharing regime in the energy sector.

For example, a similar governance concept exists in Chapter 7 of the current NER for the sharing of B2B data, that provides for the establishment of the Information Exchange Committee which is given the following regulatory functions:

- developing, consulting on and making an "Information Exchange Committee Recommendation";
- managing the ongoing development of the B2B Procedures and any changes to them; and
- establishing working groups and work programmes,

The Information Exchange Committee must have regard to the national electricity objective, B2B factors and seek to give effect to the B2B Principles when making decisions, and it requires representation of all major stakeholders such as Distribution Network Service Providers, retailers, Metering Data Coordinators, consumers, AEMO, third party B2B Participants and Discretionary Members.

It would be possible to leverage either of the governance frameworks from the DAT Act or Chapter 7 of the NER to design a suitable governance structure for data sharing in the energy industry as follows:

- **option 1**: regulatory functions could be given to the National Data Commissioner (**NDC**) to oversee the energy data sharing regime. There would be benefits to having a single data commissioner to oversee "public" data sharing, particularly around having consistency in decision making, accreditation and possibly efficiency in reducing duplication of functions. At the same time, there could be significant barriers to this, including the appropriateness of the NDC as a Commonwealth entity performing this role, the power of the NDC to do so, and the resourcing and funding of the NDS to do so; or
- **option 2**: establish, similar to the Information Exchange Committee, an energy specific public data-sharing body under the energy Rules that comprises:
  - people who are familiar with the current energy regime and the nature of energy datasets, such as representatives from the Energy Advisory Committee (which supports the Chair of the Data Standards Body for the CDR regime);
  - advisors from the ONDC or representatives from the OAIC who could contribute data-specific and technical experience; and
  - other people with relevant skills and experience.

Risk and liability

Under the DAT Bill, a data holder will be able to rely on the good faith defences under the *Freedom of Information Act 1982* (Cth) where the data holder shares data and genuinely (albeit mistakenly) believes this was authorised by the Data Sharing and Release legislation.

For example, section 56GC of the CCA includes a similar immunity for the CDR regime:

> **56GC Complying with requirements to provide CDR data: protection from liability**
>
> (1) If:
>
> (a) a CDR participant, or designated gateway, for CDR data (the ***CDR entity***):
>
> (i) provides the CDR data to another person; or
>
> (ii) otherwise allows another person access to the CDR data; and
>
> (b) the CDR entity does so, in good faith, in compliance with:
>
> (i) this Part; and
>
> (ii) regulations made for the purposes of this Part; and
>
> (iii) the consumer data rules;
>
> the CDR entity is not liable to an action or other proceeding, whether civil or criminal, for or in relation to the matter in paragraph (a).

Further, considering the issues described in sections 6 and 7 of Part B above in relation to concerns about privacy and confidential information, any disclosure of data under a DSA that is entered into

pursuant to the process set out under the data sharing framework should be deemed to be a disclosure that is at least “authorised”, and preferably “required” by or under the relevant implementing law.

Questions to consider:	
1.	**What is the appropriate governance structure for the regime?**
2.	**How should risk and liability be shared or allocated?**
3.	**Are there any concerns with disclosures of data pursuant to a DSA being deemed to be disclosures authorised or required by law?**

Appendix 1 – Glossary

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
AEMC	Australian Energy Market Commission
AEMC Establishing Act	*Australian Energy Market Commission Establishment Act 2004* (SA)
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
ARENA	Australian Renewable Energy Agency
BOM	Bureau of Meteorology
CCA	*Competition and Consumer Act 2010* (Cth)
CER	Clean Energy Regulator
CER Act	*Clean Energy Regulator Act 2011* (Cth)
CER Regulations	*Clean Energy Regulations 2018* (Cth)
CS Act	*Census and Statistics Act 1905* (Cth)
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DEE	Department of the Environment and Energy
DISER	Department of Industry, Science, Energy and Resources
DNSP	Distributed Network Supply Provider
ECA	Energy Consumers Australia
ESB	Energy Security Board
IPART	Independent Pricing and Regulatory Tribunal
MCE	Ministerial Council on Energy
MSATS	Market Settlement and Transfer Solutions

NEL	National Electricity Law
NER	National Electricity Rules
NERL	*National Energy Retail Law (South Australia) Act 2011* (SA)
NERR	National Energy Retail Rules
NGER Act	*National Greenhouse and Energy Reporting Act 2007* (SA)
NGL	National Gas Law
NGR	National Gas Rules
OAIC	Office of the Australian Information Commissioner
ONDC	Office of the National Data Commissioner

Appendix 2 – Policy and legislative reform

- National Energy Analytics Research Program, which was initiated under the 2015 National Energy Productivity Plan to enable the use of data sharing and data science to enhance energy market security, reliability, affordability and efficiency by helping to improve the accuracy of energy demand forecasts, optimise power system operations and inform wider infrastructure planning and policy.
- ACCC Retail Electricity Price Inquiry, the final report for which was released in July 2018 and found that the approach to policy, regulatory design and promotion of competition in the energy sector has not worked well for consumers and proposed a reset of the NEM and provided a plan for doing so (including 56 recommendations).
- "Big stick" legislation, by which the AER was given the right to disclose data to certain Commonwealth bodies under the *Treasury Laws Amendment (Prohibiting Energy Market Misconduct) Act 2019* (Cth) which was passed in November 2019.
- ESB Two-Sided Market Report, for which a discussion paper was released on 20 April 2020 and provides a high-level discussion on the benefits and opportunities of moving to a two-sided market and highlights how this work will be coordinated with considerations of an ahead market in the NEM.
- Establishment of National Data Commissioner to support a new data sharing framework and oversee the integrity of data sharing activities of Commonwealth agencies. We note that the National Data Commissioner has an interim role that has been established until the DAT Bill passes Parliament and receives royal assent, in its current form it does not have regulatory functions or powers as it has not yet been statutorily established.
- Release of the Department of Prime Minister and Cabinet's "Best Practice Guide to Applying Data Sharing Principles" to assist agencies holding Australian government data to safely and effectively share the data they are responsible for by using five "Data Sharing Principles".
- Release of the Data Sharing Agreement Template for consultation with stakeholders, which is a "legislation agnostic" template released in April 2020.
- CDR legislation within Part IVD of the CCA, by which consumer data held by the private sector is shared between trusted entities at the direction or authorisation of a consumer to drive greater competition and give consumers greater control and use of their own data. The implementation of the CDR regime to the energy sector is currently under consideration.
- Proposed DAT Act, which is new legislation being considered to authorise a streamlined data sharing system and encourage greater sharing of public sector data, which will strengthen data safeguards while modernising Australia's public sector data framework.

Appendix 3 – Data gaps

The responses to the RFI process identified several data gaps, where information necessary or desirable for the fulfilment of the statutory functions is not currently collected by any of the Core Bodies. These included:

1 **distribution network configuration data** – data held by DNSPs including connectivity, physics parameters and power quality measurements;

2 **operational data on Distributed Energy Resources (DER)** – currently held by manufacturers or operators;

3 **gas consumption and standing data** – data held by third party providers and network businesses of which AEMO has an inaccurate or incomplete set;

4 **early-stage development generation connection applicant data** – preliminary data on projects that may be useful for forward planning;

5 **low-voltage connectivity data** – data held by DNSPs; and

6 **consumer plan and billing data** – data held by retailers and DNSPs (and collected by the ACCC to some extent but which may not be able to be made available);

7 **ombudsman data** – data collected by jurisdictional ombudsmen;

8 **electric vehicle charger installation data** – data held by electricians not required to be provided to local licencing bodies;

9 **wholesale electricity and gas contracts market data** – including OTC and off-market trades.

Appendix 4 – General prohibitions

Body	Reference	Prohibition applies to
AEMO	s54 NEL s91G NGL ch10 NER r136 NGR	Under the NEL and NGL, AEMO must take all reasonable measures to protect "**protected information**" from unauthorised use or disclosure. Protected information is information: ▪ given to AEMO in confidence; or ▪ given to AEMO in connection with the performance of AEMO's statutory functions and classified under the Rules or the Regulations as confidential information. "**Confidential information**" under the NER and NGR is information which is or has been provided to AEMO under or in connection with the Rules (or Procedures) and which is stated under the Rules (or Procedures, in the case of the NGR), or by AEMO, the AER or the AEMC, to be confidential information or is otherwise confidential or commercially sensitive. It also includes any information which is derived from such information.
AER	ss 18 and 18D NEL s30 NGL s207 NERL s44AAF CCA	Under s 18D of the NEL, information is considered **confidential** (whether or not an express claim of confidentiality is made when the information is given) if it is obtained by the AER from a wholesale electricity supplier to assist the AER in determining whether there is effective competition within the market, there are features of the market that may be detrimental to effective competition within the market, or there are features of the market that may be impacting detrimentally on the efficient functioning of the market (and, if so, to assess the extent of the inefficiency). This information may only be used by the AER for the performance of the AER wholesale market monitoring functions or the AER wholesale market reporting functions. "**Confidential supplier information**" is defined in the NEL and means information obtained from a wholesale electricity supplier by the AER under section 18D(1)(b) that is taken to be confidential information under section 18D(2) of the NEL. The AER must not disclose confidential supplier information unless: ▪ the disclosure is for the purposes of the AER wholesale market monitoring functions or the AER wholesale market reporting functions; and ▪ the confidential supplier information has been combined or arranged with other information so that it does not reveal any confidential aspects of the confidential supplier information or identify the wholesale electricity supplier to whom the information relates. The AER's **confidentiality obligations** imported from section 44AAF of the CCA (and given effect to the NGL by s30; the NEL by s18 and the NERL by s207) require it to take all reasonable measures to protect from unauthorised use or disclosure information: ▪ given to it in confidence in, or in connection with, the performance of its functions or the exercise of its powers; or ▪ that is obtained by compulsion in the exercise of its powers.

AEMC	s24(1) and (9) AEMC EA s48 and s108 NEL s223 NERL	**Confidentiality obligations** under the AEMC EA require the AEMC to take all reasonable measures to protect from unauthorised use or disclosure information: ▪ given to it in confidence in or in connection with the performance of its functions or the exercise of its powers; or ▪ that is obtained by compulsion in exercise of its powers. The NERL imports the above confidentiality provision as if it formed part of the NERL. Further, under the AEMC EA, information that is **classified as confidential** by the AEMC under a "National Energy Law" is not liable to disclosure under the *Freedom of Information Act* 1991. National Energy Laws include the NEL, NER, NGL, NGR, NERL, NERR and regulations under those laws. Under the NEL, information provided to the AEMC for the purposes of an MCE directed review or a review conducted by the AEMC under section 45 of the NEL is **confidential information** for the purposes of Division 4 or 5 of the NEL if: ▪ the person who provides it claims, when providing it to the AEMC, that it is confidential information; and ▪ the AEMC decides that the information is confidential information. The AEMC is also restricted from publishing any information in any written submission or comment given to it under Part 7 of the NEL if: ▪ the person or body who gave the information, claims, when giving it to the AEMC, that it contains confidential information; and ▪ the AEMC decides that the written submission or comment contains confidential information.
ACCC	s95ZN CCA	Section 95ZN of the CCA applies where a person makes a claim that disclosure of the following information would **damage the competitive position** of the person: ▪ information made available, or to be made available, by or on behalf of the person (whether in oral evidence or in a written statement, submission or other document) at the hearing of an inquiry by the ACCC; ▪ information given, or contained in a document produced, by the person under section 95ZK to the ACCC. The ACCC must take all reasonable steps to ensure that this information is not disclosed, without the consent of the person, in the proceedings or by it, to a person, if the ACCC: ▪ is satisfied that the claim is justified; and ▪ is not of the opinion that disclosure of the information is necessary in the public interest.
DISER	s23 NGER Act	There is a **secrecy offence** under the NGER Act in respect of: ▪ "**greenhouse and energy information**", which is information reported to the CER under the NGER Act or the "safeguard rules" (which are rules made by the minister), or information obtained by a person whilst performing duties under the NGER Act, the regulations or the safeguard rules; and ▪ "**protected information**", which is information that:

		▪ was obtained after 2 April 2012 by a person in the person's capacity as an official of the CER; and ▪ relates to the affairs of a person other than an official of the CER. It is an offence, with a penalty of 2 years imprisonment and/or 120 penalty units, if: ▪ a person obtains greenhouse and energy information or audit information in his or her capacity as an: ▪ authorised officer; ▪ an audit team leader or audit team member; ▪ an employee of the Commonwealth, a State or a Territory or of an authority of the Commonwealth, a State or a Territory; ▪ a person appointed to an office under a law of the Commonwealth, a State or a Territory; or ▪ a person to whom information was disclosed under repealed section 26 of the NGER Act (a former provision which imposed restrictions on disclosure of certain information); and ▪ the information is not protected information; and ▪ the person discloses the information to another person otherwise than under, or for the purposes of: ▪ the NGER Act or the performance of duties in relation to the NGER Act; or ▪ the safeguard rules or the performance of duties in relation to the safeguard rules; or ▪ another law of the Commonwealth or the performance of duties in relation to another law of the Commonwealth; or ▪ if the person is an employee of a State or a Territory or of an authority of a State or a Territory, or is appointed to an office under a law of a State or a Territory—a law of that State or Territory or the performance of duties in relation to a law of that State or Territory; or ▪ if the person is an employee of the Commonwealth or of an authority of the Commonwealth, or is appointed to an office under a law of the Commonwealth—a law of a State or Territory or the performance of duties in relation to a law of a State or Territory; or ▪ if the person is an employee of the Commonwealth or of an authority of the Commonwealth or is appointed to an office under a law of the Commonwealth—advising a Minister about matters relating to greenhouse gas emissions, energy production or energy consumption.
CER	s43 CER Act	There is a **secrecy offence** under the CER in respect of "**protected information**", which is information that: ▪ was obtained after 2 April 2012 by a person in the person's capacity as an official of the CER; and ▪ relates to the affairs of a person other than an official of the CER. It is an offence, with a penalty of 2 years imprisonment and/or 120 penalty units, if: ▪ a person is, or has been, an official of the CER; and

		▪ the person has obtained protected information in the person's capacity as an official of the CER; and
		▪ the person:
		  ▪ discloses the information to another person; or
		  ▪ uses the information.

ABS	s19 and s19A CS Act	There are **secrecy offences** under the CS Act, each with a penalty of 2 years imprisonment and/or 120 penalty units, where a person commits an offence if:
		▪ the person:
		  ▪ is, or has been, the Statistician or an officer; and
		  ▪ either directly or indirectly, divulges or communicates to another person (other than the person from whom the information was obtained) any information given under the CS Act; or
		▪ the person:
		  ▪ gives an undertaking specified as a term or condition of a Ministerial determination providing for disclosure (or non-disclosure) of certain information; and
		  ▪ fails to comply with the undertaking; or
		Non-disclosure obligations apply in respect of Census information being shared with an "Agency" (which refers to a "Department", "Executive Agency" or "Statutory Agency" for the purposes of the *Public Service Act 1999* (Cth)). The obligations are that:
		▪ a person who is or has been the Statistician or an officer of the ABS must not, at any time during the period of 99 years beginning on the Census day for a Census:
		  ▪ be required to divulge or communicate to an Agency any information that is contained in a form that is given to the Statistician or an authorised officer under section 10 ("Forms to be filled up") in relation to that Census; or
		  ▪ voluntarily give such information to an Agency,
		  other than in accordance with the CS Act; and
		▪ a person who is or has been the Statistician or an officer of the ABS must not, at any time during the period of 99 years beginning on the Census day for a Census:
		  ▪ be required to divulge or communicate to a court or tribunal any information contained in a form that is given to the Statistician or an authorised officer under section 10 ("Forms to be filled up") in relation to that Census; or
		  ▪ voluntarily give such information in evidence in proceedings before a court or tribunal.

Appendix 5 – Example

AEMO Protected Information

The following steps must be taken to determine if a dataset is considered to be 'protected information' in AEMO's hands:

Step 1: Apply principle set out in legislation, see section 54(1) of NEL

> **Subdivision 1—AEMO's obligation to protect information**
>
> **54—Protected information**
>
> (1) AEMO must take all reasonable measures to protect from unauthorised use or disclosure information (***protected information***)—
>
> (a) given to it in confidence; or
>
> (b) given to it in connection with the performance of its statutory functions and classified under the Rules or the Regulations as confidential information.

Step 2: Determine if the information is classified under the Rules or the Regulations as confidential information, see definition of Confidential Information in the NER

> **confidential information**
>
> means, in relation to a *Registered Participant*, *AEMO* or a *connection applicant*, information which is or has been provided to that *Registered Participant*, *AEMO* or *connection applicant* under or in connection with the *Rules* and which is stated under the *Rules*, or by *AEMO*, the *AER* or the *AEMC*, to be *confidential information* or is otherwise confidential or commercially sensitive. It also includes any information which is derived from such information.

Step 3: Find Rule (or Rules) applicable to the dataset. There are a number of ules that classify certain electricity datasets to be Confidential Information. See Rule 7.17.3 for B2B Data

> (c) *B2B Data* is confidential information and may only be disclosed as permitted by the *Rules*.

Step 3a: Trace through relevant definition to determine if (a) dataset falls within principled definition or (b) dataset is prescribed in associated procedures or guidelines, see definition for B2B Data

B2B Data

Data relating to *B2B Communications*.

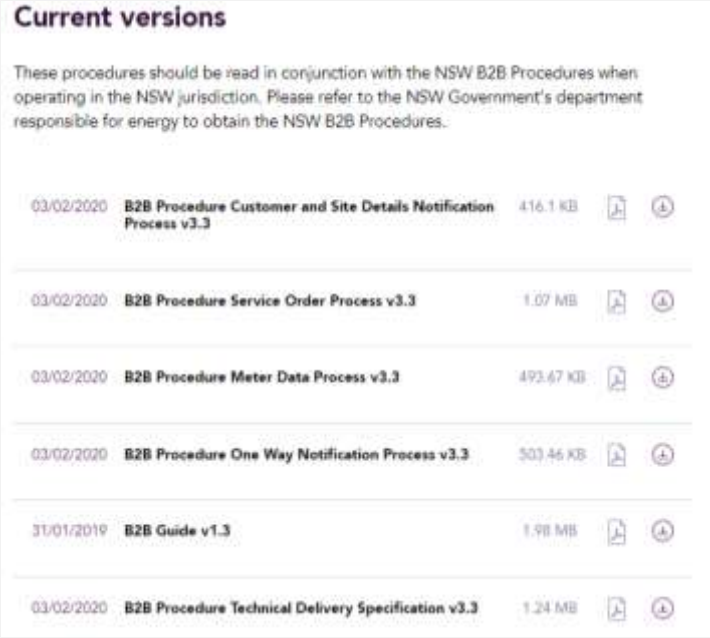
B2B Communications

Communications between *B2B Parties* relating to end-users or *supply* to end-users provided for in the *B2B Procedures*.

B2B Procedures

The *B2B Procedures* made under Part H with the content required under clause 7.17.3.

Step 3b: If the definition refers to procedures, see relevant procedures to determine if dataset is related to or provided for in the procedures. See B2B Procedures Guide (the procedures are split over 6 different documents)



Note: Procedures are not just relevant for this worked example, other relevant procedures that relate data include:

- Market Settlement and Transfer Solution Procedures (relevant to defining NMI Standing Data);
- Metering Data Provision Procedures (relevant to defining Metering Data and Energy Data); and
- Metrology Procedures (relevant to defining Metering Data).

About King & Wood Mallesons and Galexia

KWM and Galexia have established a multi-disciplinary team that provides clients with seamless strategic advice in relation to data, focussing on privacy, regulatory reform and data governance across diverse industry sectors. We have completed numerous successful projects for both government and private sector clients in areas including identity management, heath technology, data sharing, privacy protection and big data.

Disclaimer