ESB Data Strategy – Initial Reforms policy positions

This paper sets out the policy positions implemented within the proposed *National Energy Laws Amendment (Data Access) Bill 2023*, as well as related context.

These policies were developed as part of the ESB Data Strategy, Initial Reforms. Energy Ministers supported these policy positions in December 2022.

ESB has developed the resulting draft amendments bills, working with the Parliamentary Council's Committee (PCC) and the Office of the Queensland Parliamentary Council. ESB also worked closely with: advisers King & Wood Mallesons, who supported earlier legal reviews within the Data Strategy; legal advisors from all ESB market bodies and the Commonwealth Department of Climate Change, Energy, Environment and Water (DCCEEW); engagements will all jurisdictional energy departments; as well as undertaking wider public consultation.

1.3 Background / context

The ESB has been tasked by Ministers to deliver the ESB Data Strategy (agreed November 2021). Initial Reforms were identified as one of the early recommended deliverables in the strategy.

The Initial Reforms are intended to address key identified barriers to sharing data with policy makers, planners and researchers, to support more informed evidenced-based policy, particularly critical in managing the energy transition. Given urgent needs of the energy transition, these "initial" reforms are intended to be early changes, enabling safe sharing of high-value AEMO data to identified trusted parties. These reforms are proposed to be followed by a broader principles-based data sharing "New Framework", addressing data sharing barriers and protections for a wider set of data holders and users across the sector.

The ESB note that associated Data Services proposed in the Data Strategy are a critical partner enabling these Initial Reforms – providing the resources and capabilities needed to deliver data and benefits: managing agreements, protections and systems needed to facilitate release of the data, as well as supporting transparency of data available, curation, data standards and insights. ESB has consulted on and supported a governance model for Data Services, to be delivered in the near term as a Data Services Unit within AEMO, supported by a Stakeholder Advisory Group to support AEMO in targeting stakeholder needs and accessing expertise. AEMO is developing an implementation plan to proposed to jurisdictional officials, aiming to have this unit in place prior in the second half of 2023, to support services once the legislative amendments are in place.

2 Scope of Amendments

The amendments proposed in this draft legislation (Attached) seek to permit greater access to, and use of, data held by AEMO, in a secure way, for trusted policy, planning and public research bodies. References to data in these amendments refer to Protected Information as defined in the National Electricity Law (**NEL**) and the National Gas Law (**NGL**).

Specifically, draft legislative amendments to the NEL and NGL will allow (but not require) AEMO to share protected data safely with trusted "prescribed" bodies. Two categories of prescribed bodies (informally described as Class A Bodies and Class B Bodies) reflect different existing protection obligations. More explicit protection conditions are provided for Class B Bodies, including sharing limited by legislated purpose. The AER will perform an enforcement role for these initial reforms under its existing function in section 15(1)(a) of the NEL and section 27(1)(a) of the NGL.

Further amendments are included to manage AEMO's risks as it discloses protected information under the NEL and the NGL, including expanding AEMO's functions to include data sharing and supporting services, extending immunities and supporting cost recovery (where appropriate and subject to budget processes).

Non-legislative supporting measures are also proposed to improve transparency and social licence, including publishing common data sharing terms and guidelines; a public register of data sharing agreements; and potentially accreditation requirements.

3 Recommended Class A and Class B Bodies

The ESB consulted on proposed Class A and Class B bodies and worked with KWM to further review and test the existing data protection arrangements of proposed bodies.

Based on this review, the following bodies are proposed:

CLASS A BODIES	**CLASS B BODIES**
Bodies who have prescribed statutory functions either specific to the energy industry, who work with energy data for public purposes, or who are already listed in section 54C(2) of the NEL and section 91GC(2) of the NGL. Such bodies have a high level of confidence as to the security and protection of the data.	*Public bodies and researchers who can create clear benefits for energy consumers through greater access to data but require clear data protection obligations to ensure security.*
BODIES ALREADY LISTED IN SECTION 54C(2) OF THE NEL AND SECTION 91GC(2) OF THE NGL • AER; • AEMC; • ESB; • Economic Regulation Authority of Western Australia; • ACCC; • a jurisdictional regulator; • the energy ombudsman (if the information is reasonably required by an energy ombudsman to resolve a dispute between a Registered participant and a retail customer but the information is not end-use consumer information); • a prescribed body; • any staff or consultant assisting a body mentioned above in performing its functions or exercising its powers. *Additional bodies [already being implemented]* • CSIRO; • each department responsible for the administration of the application Act of a participating jurisdiction (for section 91GC(2) of the NGL);[1] and • the Ministers of the participating jurisdictions (for section 91GC(2) of the NGL)[2]. *Additional bodies under these amendments* • each department responsible for the administration of the application Act of a participating jurisdiction; • the Ministers of the participating jurisdictions; • Australian Bureau of Statistics; • Clean Energy Regulator.	• Australian universities; and research facilities that are part of an Australian university and conducting research in relation to energy; • Australian university researchers who are conducting research in relation to energy; • a prescribed body; • Energy Consumers Australia; • Australian Renewable Energy Agency; and • Clean Energy Finance Corporation.

Variations from previous proposals

A range of changes have been made to the early proposals in the consultation paper[1], in response to both issues raise by stakeholders and further review in implementation. These include:

1. **Ministers** – It is proposed that Ministers are to be included explicitly. The intent was always that the Ministers could see the data where appropriate at the discretion of their departments. However, in line with stakeholder feedback, this has now been made clear. This also aligns with changes underway for East Coast Gas Supply Adequacy[2].
2. **ARENA, CEFC, and ECA** – these bodies have been moved from Class A to Class B, where there are more explicit and transparent data protection obligations, including limits on data sharing purposes. This will give these bodies clearer guidance, aligning their arrangements with the public research bodies they engage with, and is appropriate for consumer confidence.

The draft consultation paper also included a proposal to allow the list of prescribed bodies to be amended by Ministerial Order. After further consultation with legislative drafters, it was considered that the existing mechanism to update prescribed bodies through regulation (rather than Ministerial Order) remained preferrable for transparency, ensuring that all prescribed bodies remain listed together. This will still allow the list of bodies to be updated over time.

A range of further possible expansions to access were proposed by stakeholders in the consultation process, such as expansion of information provided to the Energy Ombudsman, inclusion of a range of bodies such as local councils and community organisations, and access for wider data service providers. These organisations are diverse in their internal data protection and system capabilities. It is considered that, at this stage, benefits for this group and wider data seekers should be targeted through tailored products in the Data Services workstream. For example: dashboards for local council aggregated data; or specific data service requests to review program impacts.

The Data Strategy proposes a staged approach to reforms. This package provides only initial reforms, to build data sharing capabilities and ensure they develop robustly and securely. In line with the DATA Scheme, a second stage of reforms is expected to consider mechanisms to cover wider data holders and accredit a wider range of data users.

4 Amendments to support AEMO data sharing

A range of specific amendments aim to reduce barriers to AEMO data sharing and promote adaptability.

Expand AEMO's functions.	Expand AEMO's functions in section 49 of the NEL and section 91A of the NGL to include: • "to disclose information held by AEMO to other persons or bodies in accordance with this Law, the Rules and the Regulations". This will allow AEMO to recover its costs and give it immunity for disclosure; and

[1] Energy Security Board, *Data Strategy – Initial Reforms Consultation Paper* (July 2022), available at: https://www.datocms-assets.com/32572/1657767094-20220714-esb-data-strategy-initial-reforms-consultation-paper.pdf.

[2] *National Gas (South Australia) Amendment (East Coast Gas System) Bill 2023* (currently awaiting assent), available at: https://www.legislation.sa.gov.au/lz?path=/b/current/national%20gas%20(south%20australia)%20(east%20coast%20gas%20system)%20amendment%20bill%202023.

	• "to provide advisory and support services related to information held by, or otherwise available to, AEMO". This will facilitate AEMO providing services necessary to safely disclose data, such as de-identification and secure data delivery platforms. This could also support aspects of wider Data Services capabilities being considered by the Data Strategy[3].
Clarify AEMO's right to use information.	Amend section 53D of the NEL and section 91FD of the NGL to clarify AEMO 's right to use information, subject to anything to the contrary in the Law.
Ensure that recipients of protected information are responsible for their use and disclosure of it, not AEMO.	Amend section 54(1) of the NEL to clarify that AEMO must ensure that it does not make unauthorised use, or an unauthorised disclosure, of protected information. Allow AEMO to impose conditions to be complied with by Class B Bodies in relation to protected information that AEMO discloses to them. Restrict the purposes for which a Class B body can disclose protected information given to it by AEMO (see further below). Disclosing beyond the primary and secondary purposes may attract a civil penalty. Require Class B Bodies to take reasonable steps to protect the information from misuse, interference, loss, and unauthorised use, loss, access, modification and disclosure. Failure to do so may attract a civil penalty. Require Class B Bodies to notify the AER of any non-compliance.

5 Safeguards to support safe sharing of data

In the public consultation, several different high-level data protection and enforcement models were proposed for stakeholder comment. Based on these comments, as well as reflecting on recently proposed changes to government policy responding to recent data breaches, KWM and ESB have proposed a model that balances the need for data security and trusted data flows with increased use and disclosure of protected information in the public interest. The model aligns with the DAT Act in key respects to ensure consistency for bodies captured under both regimes, and to maintain alignment with the direction of evolving government policy.

5.3 Class A body protections

The position remains that these bodies should be constrained by their existing protection obligations. These have been further reviewed and it is considered that existing capabilities and obligations are in line with AEMO's protection capabilities, and these bodies have strong incentives to manage data conservatively and effectively.

In addition, many of these bodies are already listed as prescribed bodies and already access data through this mechanism (such as the AER and other jurisdictional regulators). Some of the protections proposed for Class B bodies discussed below could reduce existing access, which is not the intent of this package of reforms.

[3] ESB Data Services delivery model consultation paper December 2022

5.4 Class B body protections

Stakeholders and recent policy changes have highlighted the importance of clear and transparent protections for protected information, with clear incentives. This is not only to manage any risk to the protected information, but also to ensure visibility of security arrangements and consumer benefits, enhancing stakeholder comfort and social licence in use of the data for consumer benefit in the energy transition.

5.4.1 *Data sharing purposes*

In order to align with section 15(1) of the DAT Act, we consider that it is necessary for the Initial Reforms to establish data sharing purposes. It is recommended that Class B Bodies may receive data from AEMO for the following primary purposes:

Data sharing purposes – for Class B	
Proposed under the NEL and NGL 1. Delivery of government services. 2. Informing government **planning**, policy or programs. 3. Research **in connection to energy**.	*Current purposed in the DAT Act* 1. Delivery of government services. 2. Informing government policy and programs. 3. Research **and development**.

Minor changes marked above have been proposed against the DAT Act purposes, for clarity, given strong links to planning and commercial outcomes in the energy sector.

It is proposed that enforcement related purposes are a precluded purpose for Class B Bodies, which aligns with the DAT Act. Section 15(3) of the DAT Act (which is also included in the proposed reforms to the NEL and the NGL) stipulates that an enforcement related purpose means:

1. Detecting, investigating, prosecuting or punishing:
    a. an offence; or
    b. a contravention of a law punishable by a pecuniary penalty;
2. Detecting, investigating or addressing acts or practices detrimental to public revenue;
3. Detecting, investigating or remedying serious misconduct;
4. Conducting surveillance or monitoring, or intelligence-gathering activities;
5. Conducting protective or custodial activities;
6. Enforcing a law relating to the confiscation of proceeds of crime;
7. Preparing for, or conducting, proceedings before a court or tribunal or implementing a court/tribunal order.

Class B Bodies must not use or disclose the information for another purpose (a ***secondary purpose***) unless:

1. AEMO has given written consent for the use or disclosure of the information for the secondary purpose; or
2. the entity is authorised by or under another Act or law to use or disclose the information for the secondary purpose.

As discussed above, it is proposed that these data sharing purposes only apply to Class B Bodies, and **not** to Class A Bodies. This is so new constraints are not put on existing bodies who currently receive protected information from AEMO under section 54C of the NEL or section 91GC(2) of the NGL. That means that, for example, the AER will not be limited in the use of the information in accordance with its functions.

In practice, AEMO will generally require some form of agreement or MOU with Class A bodies, which identifies their purpose for requesting data. This is for transparency and as part of AEMO's discretion to ensure the data sharing remains safe. AEMO will be expected to include data detail and the purpose of Class

A body data sharing in their public data-sharing register to ensure that stakeholders have transparency over appropriate use of the data. This is in line with the public register under the DATA Scheme.

5.4.2 *Conditions on disclosure*

In order for Class B bodies to have clear protection obligations, aligned with AEMO and Class A bodies, a Class B Body must comply with the following conditions:

Conditions on disclosure – for Class B
i. **(Purpose condition)** if AEMO discloses protected information to a Class B Body for a particular purpose (the ***primary purpose***), the recipient must not use or disclose the information for another purpose (the ***secondary purpose***) unless: a. AEMO has consented to the use or disclosure of the information; or b. the recipient is authorised by or under an Act or other law to do so; and ii. **(Protection condition)** the Class B Body recipient must take such steps as are reasonable in the circumstances to protect the information: a. from misuse, interference or loss; and b. from unauthorised use, access, modification or disclosure, and ensure that the information is de-identified or destroyed when the information is no longer required; and iii. **(Reporting condition)** the Class B Body recipient must notify the AER, in an approved form (if any), of any breach of the purpose condition or the protection condition as soon as practicable, but not later than 5 business days, after the entity reasonably suspects or becomes aware that the requirement has not been complied with.

The purpose condition under paragraph (i) above requires that the Class B Body disclose to AEMO the purpose or purposes for which it wants the protected information and should have to obtain additional consent from AEMO if it later wishes to expand that purpose. This is consistent with a generally accepted privacy principle that recipients of personal information should clearly define and be limited to specific purposes for the use of that information. The secondary use and disclosure purposes are deliberately limited to purposes that AEMO has consented to, and where the recipient is authorised by or under an Act or other law to use or disclose the information.

The reporting condition in paragraph (iii) above aims to empower and minimise the AER's monitoring functions. As this applies to a limited number of recognised bodies with ongoing incentives to engage in AEMO data, a reporting condition aims to creates a material incentive to self-report. The concept of an "approved form (if any)" has been adopted from section 38 of the DAT Act. The intent here is to allow the AER to publish a form that Class B Bodies must use to notify it. This could be any form, for example a formal letter versus an online notification etc, with the intent to adapt to changing needs over time.

5.4.3 *Penalties for breach of conditions*

The Class B conditions are proposed to be subject to civil penalties. This is seen by stakeholders as critical to ensure conditions are enforced and that Class B users will invest effort in ensuring data protections are met. This makes civil penalties critical for the success of data sharing: penalties will give AEMO more confidence that they have stakeholder support and social licence to share. AEMO is very likely to limit sharing if they are uncertain of their social licence, regardless of clear legal rights and reduced direct risks, as breaching social licence is rightly perceived as a critical risk in itself. .

Note that wider non-legislative measures discussed below, including the public register of data sharing agreements and published sharing terms and guidelines, aim to further support social licence through transparency.

Tier 2 civil penalties are proposed, as described in the NEL (section 2AB(1)(b)) and specified in the Regulations. While this level of penalty is significantly more than the DAT Act (where penalties are closer to Tier 3), the magnitude of this penalty reflects:

- Alignment with the decision matrix and concept table approved by energy ministers as a decision-making framework for penalties for the AEMC to apply,[4] insofar as the relevant action by the Class B body relates to consumer data;
- the amendments permit AEMO to disclose personal *and* commercially sensitive information; and
- in response to recent breaches and growing concerns over data protection, the government has introduced amendments to the *Privacy Act 1988* which will significantly increase maximum penalties that can be applied for serious or repeated privacy breaches.[4] However, these amendments only apply to personal information. Importantly, much AEMO data can be classed as personal information. AEMO may hold information linked to an address, but not information on individual account holders (such name, ID, contact details) or businesses at that address.

Tier 2 civil penalty means:

i. if the breach is by a natural person, the penalty is—
    a. an amount not exceeding $287,000; plus
    b. an amount not exceeding $14,400 for every day during which the breach continues; and
ii. if the breach is by a body corporate, the penalty is—
    a. an amount not exceeding $1,435,000; plus
    b. an amount not exceeding $71,800 for every day during which the breach continues.

These amounts will be adjusted every three years to reflect movements in the consumer price index and published on the AER's website.

6 Enforcement

Adding NEL and NGL civil penalty provisions requires a regulator to enforce them. It has been determined that the AER is the most realistic and appropriate body to perform the enforcement role for these interim reforms where civil penalties are included. This is in large part due to the complexity of conferring this function on an alternative Commonwealth body or establishing a new entity in the short term. The AER may require additional resourcing to support it to perform this function.

The appointment of the AER as the enforcement body requires only minor amendment to the NEL.

7 Additional non-legislative controls

In addition to the above amendment to the NEL and the NGL, officials have also recognised a range of complementary non-legislative controls which are needed to be implemented by AEMO. These are aimed at reducing uncertainty for users, improving transparency and trust in data sharing, and increasing efficient in implementation. They include:

[4] See https://www.aemc.gov.au/regulation/energyrules/civil-penalty-tools.

- Publication of standard terms and conditions that apply to each class of body that may receive protected information from AEMO;

- Publication of supporting guidelines with principles and processes relating to, for example, data release, data management and curation, technical matters and standards and emerging technologies;

- A register of data AEMO has shared, to support robust tracking and compliance, as well as publicly accessible summary information to support transparency; and

- AEMO may also consider appropriate accreditation requirements for data requesters in some cases.

Work is already underway on some of these measures through the Data Strategy, including development of initial standard terms and guidelines, as well as recent consultation on supporting services required to facilitate safe data sharing.[5]

[5] See https://esb-post2025-market-design.aemc.gov.au/data-strategy#data-services-delivery-model--consultation-paper.