AUSTRALIAN ENERGY REGULATOR

Level 17, Casselden
2 Lonsdale Street
Melbourne Vic 3000

GPO Box 3131
Canberra ACT 2601

tel: (03) 9290 1800

www.aer.gov.au

Our Ref: 30777152
Your Ref: ERC0399
Contact Officer: Walter Batt Abrams
Contact Phone: 03 9290 1814

Thursday, 23 October 2025

Anna Collyer
Chair
Australian Energy Market Commission
GPO Box 2603
SYDNEY, NSW, 2001

Dear Ms Collyer,

Re: Real-time data for consumers – Draft rule determination

The Australian Energy Regulator (AER) welcomes the opportunity to respond to the Australian Energy Market Commission's (AEMC) draft determination on the National Electricity Amendment (Real-time data for consumers) Rule 2025 and National Energy Retail Amendment (Real-time data for consumers) Rule 2025.

Real-time data could bring benefits to many consumers and become an important feature of Australia's energy system in the future. While currently this data is mostly of interest to consumers using new and innovative energy services, it will become more relevant and important for a wider range of customers over time. In addition to empowering people to make more informed decisions about their own energy, it could deliver system benefits for the good of all consumers.

However, real-time data is personal information about customer behaviour and it is crucial that market participants manage and use this data safely. The draft rules could be strengthened to ensure that this information is well-protected. In this submission, we highlight some opportunities to improve protections in the draft rules for the AEMC's consideration. We also make recommendations with respect to civil penalties for a specific provision.

We encourage the AEMC to take a 'safety by design' approach to the final rules

The Essential Service Commission of Victoria's safety by design partnership has highlighted how perpetrators of family violence exploit essential services data and systems to harm customers affected by family violence. Our strategy to support a safer energy market for customers affected by family violence includes a priority to support a regulatory framework that enables safety by design to prevent essential services from being exploited by family violence perpetrators to cause harm.

Safety by design is a framework that can be used to reduce the risk of harm from the misuse of products or services, including by perpetrators of family violence. Given the ways in which personal information can be exploited to cause significant harm, a regulatory framework that

is safe by design would include the highest possible level of privacy and consent requirements for personal information as the default standard. We are pleased to see the draft rules consider arrangements for consent, revocation of access after it has been granted and protections for customers affected by family violence. Taking a safety by design approach to finalising the rules would help prevent real-time data from being weaponised.

Consent requirements should be strengthened to address risks associated with third parties

In our submission to the directions paper for this rule change, we encouraged the AEMC to consider that consent for access to real-time data could only be obtained through customer engagement with their retailer. We noted that the existing relationship between customers and retailers is the most efficient way to obtain, verify and record a customer's consent within existing systems.

Given the draft rules propose to provide customers (or their representatives) with real-time data in its raw form, there is likely to be a significant role for third-party customer representatives in managing and communicating this data. Where a third party has obtained the customer's consent to access their data as a real-time data authorised recipient, it is important that the rules require this consent to be verified and recorded by the customer's retailer. This would better ensure that access is only provided where consent has been legitimately obtained. It would also assist the AER to effectively monitor and enforce compliance with consent requirements in the draft rules.

We recommend the rules require consent for real-time data access to be handled similarly to Explicit Informed Consent under the National Energy Retail Law. Retailers should be required to maintain a verified record of the customer's consent for 2 years from the date consent was obtained. The record should be in a format and include information necessary for the AER to verify that the customer's consent is legitimate and otherwise compliant with this proposed change.

It should also be easy for customers to withdraw their consent for whatever reason they choose. The draft rules promote an environment where customers will likely access real-time data through their retailer or a third party, who will communicate the raw data in a way that makes it easier for the customer to use. However, the draft rules do not allow for customers to revoke consent through the third party. We recommend additional obligations on authorised recipients to request the retailer revoke access where the customer tells them they revoke their consent or where the authorised recipient stops providing relevant services to the customer.

The AEMC should also consider embedding appropriate and fair use protections within the new rules to make sure that real-time data is only used for purposes the customer is aware of and consents to.

Revocation of access should occur on a timeline and there should be arrangements for managing recorded data

It's important that customers have agency over their real-time data, both when it is accessed and after it becomes recorded data. This requires stronger protections in relation to revoking access.

The draft rules do not set out a timeframe for revoking access to a customer's real-time data, even though they set out a timeframe for providing it. To support monitoring and enforcing compliance with the draft rules, we recommend specifying a timeframe within which both retailers and metering coordinators must complete requests to revoke access.

Once access to real-time data has been revoked, there should be a set of obligations that govern the management of any data that may have been recorded. We suggest the rules

include a requirement for authorised recipients to either delete or permanently de-identify the data following the revocation of real-time access.

In addition, there may be situations where it is appropriate for a person who is not the small customer to request revocation of access, for example the customer's authorised representative or someone else living at the customer's premises. This would be particularly important for a person affected by family violence who is not the account holder. We recommend that the rules be drafted to ensure people who contact the retailer and are not necessarily the account holder have a pathway to enable revocation. In particular, the rules should explicitly ensure that anyone requesting revocation who is affected by family violence is protected by the timely fulfilment of their revocation request. It should be clear that this protection applies where there are indicators the person may be affected by family violence, even if they do not explicitly disclose this.

We recommend changes to draft rule 59D(1) and encourage the AEMC to recommend it be classified as a tier 1 civil penalty provision

To enable effective monitoring and enforcement, we recommend the AEMC redraft rule 59D(1) to expressly impose the obligation on retailers and metering coordinators. We also recommend that the AEMC consider drafting rule 59D(1) in a way that captures the ongoing facilitation of access in addition to the initial provision of access. We would welcome the opportunity to discuss this suggestion in more detail.

Finally, we encourage the AEMC to recommend the redrafted rule 59D(1) be classified as a tier 1 civil penalty provision.[1] This rule contains an important customer protection and a lack of associated civil penalty would limit our ability to take appropriate action in response to non-compliance. A classification of Tier 1 is consistent with other information protection provisions in the energy rules.[2]

Thank you for the opportunity to provide our feedback on the draft rules. We look forward to continuing to engage with the AEMC on this matter. If you have any questions about this submission, please contact the AER's Consumers team at consumers@aer.gov.au.

Yours sincerely,

Adam Day
Executive Director (Acting), DMO & Consumers
Consumers & Markets

Lodged online on: 23.10.2025

[1] Subject to redrafting, we consider rule 59D(1) could function as the overarching civil penalty provision that captures obligations on participants regarding consent. This would be similar to the civil penalty approach for de-energisation, in which there are two overarching civil penalty provisions (rules 107(2) and (3)) that capture retailer and distributor obligations related to de-energisation of small customers.

[2] For example, rule 76G of the Retail Rules and clause 8.6.1 of the Electricity Rules.