

AEMO Privacy Policy

Board-Approved Policy Document

Purpose

Australian Energy Market Operator Limited (**AEMO**) values and is committed to protecting the privacy of individuals, and complying with its obligations under the *Privacy Act 1988 (Cth)* (**Privacy Act**) and the Australian Privacy Principles in Schedule 1 to the Privacy Act. This policy explains how AEMO will manage personal information.

Policy Requirements

Why AEMO collects and holds personal information

1. AEMO will only collect and hold personal information where necessary for AEMO's operations, including for the performance of its statutory functions and services. This may include personal information provided:
 - in the course of AEMO's energy market and system operations, and national transmission planning
 - to assist in managing business and stakeholder relationships including personal information about individuals representing participants and industry associations in the energy industry
 - in connection with services acquired or provided by AEMO
 - for employment purposes, including potential employees who voluntarily provide their résumé and identification documents to AEMO
 - to ensure compliance with any relevant law
 - during a situation that involves a threat to health and safety
 - in a dispute resolution process, or for the purposes of a person establishing, exercising or defending a legal or equitable claim.
2. Without this information, AEMO may be limited in how it can perform its services and engage with an individual (including responding to queries or requests submitted to AEMO).

Types of personal information AEMO may collect and hold

3. The kinds of personal information AEMO collects and holds will vary depending on the purpose for its collection and may include:
 - identifying information (such as a name and date of birth)
 - contact information (email address)
 - usernames and passwords for accounts created with AEMO
 - records of communications (including messages sent to AEMO)
 - device information (e.g. IP address).

4. Sensitive information is defined in the Privacy Act, and includes things like racial or ethnic origin, biometric and health information. Where an individual is an employee or contractor of AEMO, AEMO may also collect sensitive information (for example in photos and biometrics used for security identification, or for health and safety purposes). If we are legally required to do so, we will ask the relevant individual for their consent beforehand.

How AEMO collects and holds personal information

5. AEMO may collect information from a variety of sources. Generally, *personal information* is provided:
- directly and voluntarily by the relevant individual through AEMO's website, by telephone, in person or by other communication
 - by a person's employer, or an organisation the person represents, to AEMO for the purposes of registration for participation or training in an energy market operated by AEMO
 - by another person, to AEMO for the purposes of AEMO performing its functions and exercising its powers in relation to an energy market it operates.

Cookies and links to third party websites

6. AEMO's website makes use of cookies to collect information about interactions with AEMO's website and to provide users with a more effective or tailored service. "Cookies" are small text files created and stored on a computer hard drive by the internet browser software to hold relevant information about a website. If this is of concern, individuals may check their web browser's help menu to see if cookies may be disabled.
7. AEMO's website may contain links to third party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data. These websites have their own privacy notices or policies and AEMO does not accept any responsibility or liability for their data processing activities.

Storage and security of personal information

8. AEMO takes reasonable steps to ensure that the personal information it collects is stored in a secure environment protected from misuse, interference, loss, unauthorised access, modification or disclosure. We regularly assess the risks of misuse, interference, loss, unauthorised access, modification or disclosure of personal information, and ensure that we have adequate technical and organisational measures in place to address those risks, including staff training, policies, procedures and technology.
9. AEMO also takes reasonable steps to destroy or permanently de-identify personal information that AEMO no longer needs and is not legally required to retain.

How AEMO may use and disclose personal information

10. AEMO will use and disclose personal information for the purpose for which it was collected.
11. AEMO may also use or disclose personal information for a related purpose if that use or disclosure would be reasonably expected by the relevant individual. Examples of such situations include the use or disclosure of personal information:
- to advise of training or services that may be of interest (individuals can opt-in to receive marketing)
 - to conduct a stakeholder satisfaction survey to improve performance of AEMO's functions and services
 - to investigate or prevent any suspected or alleged breach of applicable laws, rules or procedures

- for any other purpose that AEMO expressly states at the time of collection
- to address a situation that involves a threat to health and safety.

12. AEMO may also use or disclose personal information with the consent of the relevant individual.

13. Sometimes AEMO may need to disclose personal information to third parties, such as:

- referees, representatives and other people an individual has authorised AEMO to interact with, on their behalf
- professional advisers who AEMO engages to provide advice
- service providers AEMO engages for the purpose of performing its functions
- debt collection agencies
- law enforcement bodies and national security agencies
- other regulatory bodies and government agencies or other people as required by law.

Disclosure of personal information to overseas recipients

14. AEMO may occasionally need to disclose personal information to a person located overseas who may be subject to different privacy regimes. This may include service providers who manage a process for AEMO, such as quality assurance analysis of information, IT vendors and support centre calls. Overseas locations in which an individual's information may be shared include United Kingdom, the European Union and the United States of America.

Automated Decision-Making

15. We may use third party platforms or computer programs including artificial intelligence (AI) to process an individual's personal information for the purposes described in this policy, subject to the security measures described at sections 8 and 9 of this policy. Such processing may include:

- creation of transcripts and summaries of events and meetings
- providing personalised products or services
- analysis of survey results and feedback (such as industry analysis)
- developing insights to support and improve the performance of our functions and services.

16. Where decisions using such platforms or computer programs could reasonably be expected to significantly affect an individual's rights or interest, AEMO's process incorporates additional safeguards such as having AEMO personnel review and assess the AI-outputs or recommendations. Any concerns about the use of AI in relation to personal information, may be directed to AEMO as set out in section 20.

How individuals can access and correct their personal information

17. An individual can request access to any personal information AEMO holds about them, by contacting AEMO as set out in section 20. AEMO aims to respond within 30 days and provide access to the information in the manner requested, if it is reasonable and practicable to do so. AEMO is entitled to refuse the request to access personal information in some circumstances, for example where:

- access may pose a threat to other individuals or unreasonably affect their privacy
- refusal is authorised or required by law or court order
- access would disclose commercially sensitive information
- access is likely to prejudice enforcement activities by an enforcement body

- the request is frivolous or vexatious.

18. There is no charge for access to an individual's own personal information.

19. AEMO tries to ensure that personal information in its possession is accurate, up-to-date, complete, relevant and not misleading. A request for AEMO to correct an individual's personal information may be directed to AEMO as set out in section 20, and AEMO will take all reasonable steps to correct the information within 30 days. If AEMO cannot correct the information, AEMO will provide a written notice explaining the reasons.

Enquiries or complaints

20. For more information or to submit a request or complaint about the way AEMO manages personal information, (including a request to access or correct personal information or to opt out of receiving marketing or promotional material from AEMO), please email privacy@aemo.com.au or contact AEMO's Information & Support Hub on 1300 236 600 with relevant details and the subject **Attn Privacy Officer**.

21. In respect of a complaint about a potential breach by AEMO of the Australian Privacy Principles, AEMO will investigate the complaint and endeavour to respond in writing within 30 days. The response will explain whether AEMO considers that it has breached an Australian Privacy Principle and, if so, AEMO's proposed course of action. If a response from AEMO is not received within 30 days, or if AEMO's response is otherwise unsatisfactory, a complaint may be made to the Office of the Australian Information Commissioner (OAIC) via its website at www.oaic.gov.au.

Changes to this policy

22. AEMO may make changes to this policy from time to time, to take into account changes to AEMO's standard practices and procedures or where necessary to comply with new laws and regulations. The latest version of this policy will always be available on AEMO's website.