

Privacy Collection Notice - Biometric Information

This notice explains how Australian Energy Market Operator Limited (AEMO) handles your personal information, when it includes your biometric information such as fingerprint templates, facial recognition data, or other biometric identifiers. It should be read together with the [AEMO Privacy Policy](#), which explains more generally how AEMO manages personal information, including access, correction and complaints.

Why is your biometric information being collected?

As part of managing secure access to AEMO facilities and systems, AEMO may at times be required to collect and use your biometric information. Biometric information may be used for identity verification and access control purposes, such as using fingerprint information to create and enable an individual access card for secure entry to AEMO-controlled facilities, including designated data centres.

Biometric information is sensitive information under the *Privacy Act 1988 (Cth)* and will be handled with appropriate safeguards and in accordance with the [AEMO Privacy Policy](#), and the Australian Privacy Principles. AEMO seeks your consent before collecting it.

How do we handle your biometric information?

The fingerprint information is provided directly by you when you attend the designated AEMO-controlled facility. An authorised administrator uses a scanner to enrol the fingerprint and create the encrypted biometric template for your individual access card. The fingerprint information is used only to authenticate the cardholder at biometric-enabled access points and support physical security controls.

Biometric information may also be used to support security, safety, and operational requirements and to meet AEMO's regulatory, contractual, and critical infrastructure security obligations. It will be stored securely using technical and organisational security controls designed to prevent misuse, interference, loss, unauthorised access, modification or disclosure.

Access to biometric information will be restricted to authorised personnel and approved service providers who require access to perform their duties. AEMO may disclose biometric information to a person located overseas who may be subject to different privacy regimes and AEMO will take reasonable steps to ensure appropriate protections are in place. Where AEMO engages third-party providers to support biometric systems, those providers will be required by AEMO to implement appropriate privacy, confidentiality, and security protections.

AEMO will retain biometric information only for as long as it is required for the purpose for which it was collected, or as otherwise required by law. Once no longer required, the information will be securely destroyed or permanently de-identified.

What happens if you do not consent?

You are not required to consent to the collection of your fingerprint or other biometric information. However, if you do not consent, AEMO may be unable to provide you with access to facilities, systems or assets where biometric authentication is required.

How to access, correct, enquire or complain about your personal information?

You may request access to or correction of your personal information or withdraw your consent to the collection and use of your biometric information, by contacting the AEMO Security or Facilities representative who arranged your access. Withdrawal of consent may affect your ability to access facilities, systems or assets where biometric authentication is required.

The [AEMO Privacy Policy](#) also explains how to request access to or correction of personal information held by AEMO, how to make a privacy enquiry or complaint, and how AEMO will deal with a complaint. You may contact AEMO at privacy@aemo.com.au or the Information & Support Hub on 1300 236 600 (Attn Privacy Officer).