# New privacy laws and the Cloud - blueAPACHE

Canonical: https://www.blueapache.com/blog/new-privacy-laws-and-the-cloud-2

## Details:

Historical context: this article discusses Australia's March 2014 privacy reforms. Its historical penalty figures and cloud descriptions are not statements of current law or every current service configuration. The reforms introduced the Australian Privacy Principles for covered entities. The original article reported civil penalty figures of up to $340,000 for individuals and $1.7 million for companies in relation to serious privacy breaches. These are historical figures from that article, not current penalty limits. Australian organisations should already have their houses in order by building privacy and data protection in the design specifications and architectures of their IT systems to facilitate compliance. Under Australian Privacy Principle 8, before an APP entity discloses personal information to an overseas recipient it generally must take reasonable steps to ensure the recipient does not breach the APPs other than APP 1. Exceptions apply, as explained in the OAIC guidance. The challenge with overseas data centres or cloud providers (or local companies that aggregate or resell overseas cloud products) will be ensuring contracts are robust enough to ensure the data is going to be handled in accordance with Australian Privacy Principles. The OAIC explains that disclosure involves making personal information accessible outside the entity and releasing its subsequent handling from effective control. Overseas storage is not automatically a breach: in limited circumstances, a tightly controlled cloud-storage arrangement may be a use rather than a disclosure. See OAIC Chapter 8 . The original article also raised concerns about foreign-law access to data. Assess jurisdiction, access arrangements and legal obligations for the particular service rather than treating the historical discussion as current legal advice. The original article described its emPOWER Cloud offering as Australian-hosted with no overseas storage, replication or backup. For a current deployment, confirm the primary, backup, disaster-recovery and support-access locations in the agreed service scope. See emPOWER Cloud . For current guidance, see the Australian Privacy Principles guidelines (current OAIC guidance) . This link provides current guidance rather than the original historical announcement. To better understand your data privacy compliance requirements or to learn more about our emPOWER Cloud, contact our Account Management team.

### *When did the new privacy laws in Australia mentioned in this blueAPACHE article take effect?*

The article discusses the privacy reforms that took effect on 12 March 2014 and introduced the Australian Privacy Principles for covered entities.

### *What historical penalty figures did the article report?*

The article reported up to $340,000 for individuals and $1.7 million for companies. Those are historical figures, not current penalty limits.

### *What does Australian Privacy Principle 8 require of entities regarding overseas data recipients?*

APP 8 generally requires an APP entity to take reasonable steps before disclosing personal information overseas to ensure the recipient does not breach the APPs other than APP 1. Exceptions apply; the OAIC guidelines explain them.

### *According to the Office of the Australian Information Commissioner (OAIC), when does a 'disclosure' of information occur?*

OAIC guidance describes disclosure as making information accessible outside the entity and releasing its subsequent handling from effective control. Overseas storage is not automatically a breach, and some limited cloud-storage arrangements may be a use rather than a disclosure.

### *Who should be contacted to learn more about your emPOWER Cloud or data privacy compliance requirements?*

Readers are advised to contact our Account Management team to better understand their data privacy compliance requirements or to learn more about emPOWER Cloud.