

Australia's Privacy Act and Australian Privacy Principles

FAQs

Last Updated: 09.29.2023

1. What is the Privacy Act and the APPs?

The *Privacy Act 1988* (Cth) (**Privacy Act**) is Australia's primary data protection law. The Privacy Act contains the Australian Privacy Principles (**APPs**), which set out the main requirements in relation to the collection, use, and disclosure of personal information in Australia. State and territory privacy laws also apply.

The Privacy Act was most recently amended in December 2022 by the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (**Amendment Act**), which introduced increased penalties for non-compliance, and expanded the scope of the Privacy Act's extra-territorial application. The Privacy Act is also undergoing review by the Commonwealth Attorney-General's Department with the view of modernizing the law to ensure that it is fit for purpose in the digital age. It is anticipated that major changes to the Privacy Act will be introduced in the near future to implement the recommendations from the review.

The Privacy Act is enforced and administered by the Office of the Australian Information Commissioner (**OAIC**), a government agency which oversees compliance with the Privacy Act and is responsible for investigating potential breaches of the Privacy Act (amongst other responsibilities). The OAIC also publishes guidance documents to assist organisations with interpreting their obligations under the Privacy Act and the APPs.

2. What changes were introduced by the Amendment Act?

The Amendment Act increased the maximum penalty for serious and repeated interferences with an individual's privacy substantially from AU\$2.22 million to the greater of:

- AU\$50 million; or
- if a court can determine the value of the benefit that the organization or its related entities, have obtained and that is reasonably attributable to the violation —3 times the value of that benefit; or
- if the court cannot determine the value of that benefit—30% of the adjusted turnover of the organization during the 'breach turnover period' for the contravention.

The Amendment Act also lowered the threshold for a foreign organization to be covered by the Privacy Act. Prior to the Amendment Act, an 'Australian link' required the elements of: (i) carrying on business in Australia and (ii) collecting or holding personal information in Australia. The amendments to subsection 5B(3) of the Privacy Act now only require (i) carrying on business in Australia to establish an "Australian link" (described in the question below).

Lastly, the Amendment Act expanded the enforcement and information sharing powers of the OAIC, including new powers to request information and assess whether an organization has complied with its obligations to report notifiable data breaches, to share information regarding breaches of the Privacy Act with other regulators, and to disclose information to the public where it is in the public interest to do so.

3. What is the territorial scope of the Privacy Act?

As noted above, the Privacy Act applies extraterritorially if the foreign organization has an 'Australian link' and 'carries on' business in Australia. Whether an organization 'carries on' business in Australia is a fact-specific analysis. Generally speaking, an organization carries on business 'in Australia' if there is some systematic and regular activity in Australia with a view to profit that forms part of the organizations business, even if the bulk of its commercial activities take place overseas and it has no physical presence in Australia.

4. What does it mean to process personal information?

"Personal information" is defined under the Privacy Act to broadly mean information or an opinion about an identified individual, or an individual who is reasonably identifiable.

The Privacy Act does not use the term "processing", and instead refers to personal information being "collected", "used", or "disclosed". An entity "collects" personal information if it collects personal information for inclusion in a record (which includes any document, or electronic or other device).

The terms "use" and "disclosure" are not defined in the Privacy Act. According to the OAIC's guidance, the terms generally have the following meanings:

- An entity "uses" personal information when it handles and manages information within the entity's effective control.
- An entity "discloses" personal information when it makes accessible or visible to others outside the entity and release the subsequent handling of personal information from its effective control.

5. What rights do individuals have under the Privacy Act and how will Autodesk support these rights?

The Privacy Act provides the following rights to individuals in relation to their personal information:

- right to be notified of the collection of their personal information;
- right to not identify themselves or to use a pseudonym when dealing with an APP entity;
- right to request access to their personal information; and
- right to seek correction of their personal information.

Individuals may also submit complaints regarding the handling of their personal information to APP entities that handle their personal information. If they are not satisfied with the how the APP entity handles their complaint, they may also make a complaint to the OAIC.

6. Does the Privacy Act require personal information to stay in Australia?

The Privacy Act does not contain a data localization requirement, meaning that personal information is not required to be kept in Australia.

However, the transfer of personal information out of Australia is subject to safeguards. Cross-border transfers are permitted if an APP entity takes reasonable steps to ensure that overseas recipients of personal information do not breach the APPs in relation to the information (unless an exception applies). In practice, this may include measures such as entering into contracts that contain terms to the effect that the overseas recipient will comply with the requirements of the Privacy Act and APPs.

An APP entity may also disclose personal information to an overseas recipient in certain other circumstances such as (amongst others):

- if the entity reasonably believes that the recipient of the information is subject to a law, or binding scheme that has the effect of protecting the information in a way that, overall, is at least substantially similar to the protections of the APPs; or
- the individual consents to the disclosure; or
- a permitted situation under the Privacy Act exists.

7. Does the Privacy Act create special rules for minors?

The Privacy Act does not create special rules for minors. However, where the Privacy Act requires consent from an individual in order to collect, use or disclose personal information, consent will be determined on a case by case basis. Where a minor does not have capacity to provide consent, parental consent will be relied on instead.

8. How will Autodesk demonstrate compliance with the Privacy Act?

We are committed to practicing transparency in how we handle personal information. We conduct internal assessments to maintain our obligations under the Privacy Act. For additional information, please visit our [Trust Center](#). You can find our Global Privacy Statement [here](#).

9. How can I contact Autodesk's Australian affiliate?

The contact information for Autodesk's Australian entity is:

Autodesk Australia Pty Ltd
Spaces Level 17, 1 Denison Street, North Sydney
NSW 2060, Australia