Overview

This document does not provide legal advice and the information we present may not take into account future changes in laws and regulations. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

What services does Salesforce offer?

Salesforce is the leading provider of enterprise cloud computing technologies. ‘Cloud computing’ is a broad term but generally denotes a range of IT services provided in various formats through social, mobile and open technologies.

Salesforce enables companies to place their customers at the heart of their business and engage with them in new and powerful ways. Salesforce services include customer relationship management (CRM), collaboration, and social media monitoring for businesses of all sizes. Salesforce also provides platforms to build and run business applications without having to invest in new software, hardware, or related infrastructure. More information on the types of products and services that Salesforce offers can be found on the Salesforce website.

How does Salesforce deliver its services?

Salesforce generally delivers its services via the Internet. Customers log into Salesforce’s services through a website using unique usernames and passwords. Salesforce’s services allow for various additional authentication methods that may be activated by customers, as appropriate to their needs, such as two-factor authentication and IP range restrictions. We also serve our customers through what is known in the industry as cloud-based services architecture, which is designed for security, efficiency, availability, scalability, and rapid innovation.

Does Salesforce comply with Australian Privacy Laws?

Yes. Salesforce complies with the Privacy Act as such laws apply to Salesforce in its role as a service provider provisioning and operating Salesforce’s services.

Does the Privacy Act allow personal information to be transferred outside of Australia?
Yes. Australian Privacy Principle 8 (APP 8) governs the cross-border disclosure of personal information and sets out the obligations an entity is subject to, or the exceptions available to them, in the event the entity discloses personal information to a recipient located outside of Australia. The guidance relevantly clarifies the distinction between a ‘disclosure’ and a ‘use’.

Specifically, the Office of the Australian Information Commissioner’s (OAIC) guidance indicates that APP 8 applies when the personal information is disclosed by an entity and thereby makes the information “accessible to others outside the entity and releases the subsequent handling of the information from its effective control” [emphasis added].

In contrast, the guidance indicates that where an Australian entity does not release the subsequent handling of the personal information from its effective control, providing personal information to a recipient located outside of Australia may be considered a ‘use’ and therefore not subject to the obligations set out in APP 8.

The guidance gives the example where an Australian entity provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the entity may access the personal information and indicates this may be considered a ‘use’ where the parties enter into a contract that:

(i) requires the service provider only to handle the information for limited purposes;
(ii) gives the Australian entity effective control of how the personal information is handled by the overseas recipient such as by giving the Australian entity the power to access, change, or retrieve the personal information; sets out who will be able to access the personal information and for what purposes; includes the types of security measures that will be provided; and by ensuring the personal information can be retrieved and/or permanently deleted by the entity when no longer required or at the end of the contract; and
(iii) requires the service provider to enter into the same obligations with any subcontractor with access to the personal information.¹

As Salesforce processes personal information only as instructed by its customers for the following purposes (i) processing in accordance with the agreement and applicable order form(s); (ii) processing initiated by the customer’s users in their use of the services; and (iii) processing to comply with other documented reasonable instructions provided by the customer (e.g., via email) where such instructions are consistent with the terms of the agreement. Salesforce’s customers solely determine what personal information is submitted to and processed by Salesforce’s services and therefore retain effective control over the personal information they input into our services.

In which countries does Salesforce store its customer’s data?

How does Salesforce help customers ensure compliance with their Australian privacy obligations in their use of Salesforce’s services?
Salesforce has implemented procedures designed to ensure that personal information is processed only as instructed by the customer.

Additionally, upon request Salesforce makes available to its customers a data processing addendum that is tailored to address applicable requirements of global privacy laws, including the Privacy Act. The standard data processing addendum is publicly available here. Salesforce’s data processing addendum includes (i) an obligation for Salesforce to only use and disclose personal information in accordance with customers’ instructions; (ii) assurances to assist in the exercise of rights by individuals whose personal information is processed by Salesforce; (iii) provisions related to Salesforce’s personnel; (iv) obligations regarding subprocessors that may be engaged by Salesforce; (v) information about Salesforce’s security controls; (vi) security breach notification requirements; (vii) provisions relating to Salesforce’s cross-border transfer frameworks; and (viii) information about Salesforce’s return and deletion of data submitted by customers.

**How does Salesforce support customers to meet their obligations under the Notifiable Data Breaches scheme?**

In February 2018, the Australian Notifiable Data Breaches scheme commenced which introduced notification obligations on entities when a data breach is likely to result in serious harm to any individual’s whose personal information has been breached.

Salesforce commits to providing notification to our customers in the event we become aware of an incident which has resulted in the loss, unauthorised disclosure or access to our customer’s data, including personal information.

This supports our customers to determine whether an ‘eligible data breach’ has occurred and the notification obligations under the scheme may be triggered.

**How does Salesforce help protect its customer’s data?**

Salesforce has a robust and comprehensive privacy and security program addressing the use, disclosure, and protection of its customer’s data. Salesforce has implemented an array of technical measures to help secure its services and offers its customers a wide array of configurations and tools to implement in their use of Salesforce’s services to further protect its customer’s data. Multiple third parties regularly certify, validate, and audit Salesforce’s information technology and privacy measures and controls. For further details on Salesforce’s privacy and security program, please see the Security, Privacy, and Architecture Documentation, available for each service through the Trust and Compliance Documentation available at [https://trust.salesforce.com/en/trust-and-compliance-documentation](https://trust.salesforce.com/en/trust-and-compliance-documentation).