

APRA Prudential Standard CPS 231 and Okta

Institutions regulated by the Australian Prudential Regulation Authority (“APRA”) must comply with Prudential Standard CPS 231 Outsourcing (“CPS 231”) when outsourcing a material business activity. A material business activity is “one that has the potential, if disrupted, to have a significant impact on the APRA-regulated institution’s or group’s business operations or its ability to manage risks effectively,”

taking into account a variety of factors. The regulated institution must determine what it considers a material business activity.

This document is designed to help institutions regulated by APRA consider CPS 231 in the context of using the Okta Service, focusing on paragraphs 28 to 30 of CPS 231 (The Outsourcing Agreement).

CPS 231 Provisions

Okta Commentary

28. Each outsourcing arrangement must be contained in a documented legally binding agreement, except where otherwise provided in this Prudential Standard. The agreement must be signed by all parties to it before the outsourcing arrangement commences.

Okta’s Master Subscription Agreement is executed by the parties and governs Customer’s subscription to the Okta Service. See Okta’s current terms at www.okta.com/terms.

29. At a minimum, the agreement (including arrangements with related bodies corporate) must address the following matters:

(a) the scope of the arrangement and services to be supplied;

The Master Subscription Agreement will be accompanied by an Order Form which specifies the services and products purchased by a Customer and is governed by the terms and conditions of the Master Subscription Agreement.

(b) commencement and end dates;

The Master Subscription Agreement and Order Form provide details about commencement, renewal, and termination of a subscription Term.

(c) review provisions;

Okta makes a number of resources available to help Customers review and understand Okta’s formal security program on an ongoing basis, including:

- Okta’s most recently completed independent Audit Report (as defined in the Master Subscription Agreement) which is available upon request under a non-disclosure agreement.
- Trust and Compliance Documentation
- Security Technical Whitepaper
- The Trust site, which lists Okta’s other certifications such as ISO 27001
- Asia-Pacific Economic Cooperation Privacy Recognition for Processors certification (available [here](#))

CPS 231 Provisions

Okta Commentary

(d) pricing and fee structure;

A Customer's Order Form provides details about pricing and fee structure.

(e) service levels and performance requirements;

The Okta Service's historical and current performance may be reviewed on the [Trust](#) site.

(f) the form in which data is to be kept and clear provisions identifying ownership and control of data;

Form: Okta protects Customer Data as described in the Security & Privacy Documentation available on the [Trust and Compliance](#) page.

Ownership: Customers own their Customer Data, as described in the [Master Subscription Agreement](#).

Control: Okta's Customers provide Okta a limited license to use Customer Data, as reasonably necessary for Okta to provide the Service in accordance with the [Master Subscription Agreement](#). Moreover, Okta's Data Processing Addendum, available on the [Trust and Compliance](#) page, outlines how Okta processes Personal Data in accordance with Customer's documented instructions.

(g) reporting requirements, including content and frequency of reporting;

Okta notifies Customers about security incidents without undue delay as described in the Data Processing Addendum and Security & Privacy Documentation, which is available at [on the Trust and Compliance](#) page.

(h) audit and monitoring procedures;

Okta's Data Processing Addendum provides an audit procedure in accordance with the Standard Contractual Clauses. In addition, Customers may monitor Okta's practices on an ongoing basis as described above under "review provisions."

(i) business continuity management;

The [Master Subscription Agreement](#) incorporates the [Trust and Compliance](#) Documentation, which includes the Security & Privacy Documentation. The Security & Privacy Documentation contains information about Okta's disaster recovery plan, including business continuity.

(j) confidentiality, privacy and security of information;

The [Master Subscription Agreement](#) incorporates the [Trust and Compliance](#) Documentation, which includes the Security & Privacy Documentation. Customers may also execute a Data Processing Addendum, which is also available on the [Trust and Compliance](#) page. These documents contain information about how Okta protects the confidentiality, privacy, and security of our Customers' data.

(k) default arrangements and termination provisions;

The [Master Subscription Agreement](#) contains terms regarding default arrangements and termination provisions.

(l) dispute resolution arrangements;

The [Master Subscription Agreement](#) contains terms regarding dispute resolution arrangements.

CPS 231 Provisions

Okta Commentary

(m) liability and indemnity;

The Master Subscription Agreement between Okta and Customer contains liability and indemnity terms.

(n) sub-contracting;

Okta provides our Customers with information regarding our sub-processors to help them assess risk. Our Data Processing Addendum and our Sub-processor Information document, both available on the Trust and Compliance page, provide details about Okta's sub-processors and how our Customers can subscribe to receive notification of a change to Okta's sub-processors.

(o) insurance; and

Okta maintains insurance coverage against a number of identified risks.

(p) to the extent applicable, offshoring arrangements (including through subcontracting).

Okta's Data Processing Addendum and our Sub-processor Information document, both available on the Trust and Compliance page, provide details about the location(s) where data processing occurs.

Customers who are interested in learning about Okta environments in certain geographies should speak with their sales representative.

30. An APRA-regulated institution that outsources a material business activity must ensure that its outsourcing agreement includes an indemnity to the effect that any sub-contracting by a third party service provider of the outsourced function will be the responsibility of the third party service provider, including liability for any failure on the part of the sub-contractor.

Okta requires that our sub-processors meet the same high standards that we do. Okta provides our Customers with information regarding our sub-processors to help them assess risk. Okta's Data Processing Addendum provides that Okta will remain liable for the acts and omissions of its sub-processors, and Okta's Sub-processor Information document provides details about Okta's sub-processors.

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.