

Australian Privacy Act / Australian Privacy Principles — Compliance Attestation

Introduction

This document constitutes Akka's formal attestation of compliance with the Australian Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) issued thereunder. It is intended for customers, prospects, and auditors seeking assurance about Akka's personal information handling practices as they relate to Australian individuals.

This attestation is made by Akka's Chief Information Security Officer and reflects the state of Akka's privacy programme as of the date shown below. It is subject to annual review.

Scope

Akka Technologies, Inc. ("Akka") is a US-headquartered technology company providing the Akka platform — a reactive microservices and distributed systems toolkit — as both a SaaS offering and open-source SDKs. Akka collects, holds, uses, and discloses personal information of Australian individuals in the course of:

- Operating its SaaS platform and developer portals accessed by Australian customers and developers
- Managing commercial relationships with Australian enterprise customers
- Processing contact information, account data, and usage data for Australian users

As a commercial operator handling personal information of Australian individuals, Akka meets the definition of an APP entity and is subject to all 13 Australian Privacy Principles.

Compliance Posture

Akka has implemented a comprehensive privacy programme aligned with the 13 Australian Privacy Principles. As of the attestation date:

- Total controls: 15
- Controls Implemented: 15 (100%)
- Controls Not Applicable: 0
- Overall risk profile: All controls rated Low risk
- Compliance status: Compliant

Akka maintains an ISO 27001-aligned Information Security Management System (ISMS) that encompasses privacy controls across the full data lifecycle — collection, use, storage, disclosure, and disposal.

Key Controls

APP 1 — Open and Transparent Management of Personal Information

Akka maintains a publicly available Privacy Policy that clearly describes what personal information is collected, the purposes for collection, how the information is used and disclosed, how individuals can access and correct their information, and how to make a privacy complaint. The Privacy Policy is reviewed annually and updated whenever material changes occur to Akka's data handling practices.

APP 2 — Anonymity and Pseudonymity

Where practicable, Akka provides individuals with the option to interact anonymously or under a pseudonym. Developer access to open-source documentation and community resources does not require registration with real-name personal information.

APP 3 and APP 4 — Collection of Solicited and Unsolicited Personal Information

Akka collects personal information only where it is reasonably necessary for one or more of its functions or activities. Collection is limited to what is needed for account management, platform operation, customer support, and contractual purposes. Unsolicited personal information that does not meet the collection threshold is destroyed or de-identified promptly.

APP 5 — Notification of Collection

At or before the time of collection, or as soon as practicable afterwards, Akka notifies individuals of the matters required by APP 5, including the identity of the collecting entity, the purposes of collection, any third parties to whom the information may be disclosed, and the individual's rights of access and correction. This notification is delivered through Akka's Privacy Policy and in-product consent flows.

APP 6 — Use and Disclosure of Personal Information

Personal information collected by Akka is used and disclosed only for the primary purpose for which it was collected, or for a secondary purpose where an exception under APP 6 applies (including with individual consent). Akka does not sell personal information to third parties.

APP 7 — Direct Marketing

Akka's direct marketing activities comply with APP 7. Individuals are provided with a clear and easy mechanism to opt out of direct marketing at all times. Marketing lists are maintained with documented consent records, and opt-out requests are actioned promptly.

APP 8 — Cross-Border Disclosure

Prior to disclosing personal information to overseas recipients (including cloud infrastructure providers), Akka takes reasonable steps to ensure the recipient does not breach the APPs. Akka's primary cloud infrastructure providers (Amazon Web Services and Google Cloud Platform) are contractually bound to data protection standards consistent with the APPs and hold current SOC 2 Type II certifications. Data Processing Agreements are in place with all significant overseas processors.

APP 9 — Adoption, Use, or Disclosure of Government Related Identifiers

Akka does not adopt, use, or disclose Australian government-related identifiers (such as Tax File Numbers or Medicare numbers) as its own identifiers, nor does it collect such identifiers in the ordinary course of its operations.

APP 10 — Quality of Personal Information

Akka takes reasonable steps to ensure the personal information it holds is accurate, up-to-date, and complete. Customers are provided with self-service tools to update their account information, and Akka's support processes include procedures for correcting inaccurate records on request.

APP 11 — Security of Personal Information

Akka implements technical and organisational security measures appropriate to the sensitivity of the personal information held. These measures include:

- Encryption of personal data at rest (AES-256) and in transit (TLS 1.2+)
- Role-based access controls and least-privilege principles
- Multi-factor authentication for all internal systems
- Continuous vulnerability management and penetration testing
- Incident response procedures with defined notification timelines
- Employee security awareness training

AWS and GCP infrastructure security is validated by their SOC 2 Type II reports, copies of which are available to Akka customers upon request.

APP 12 — Access to Personal Information

Individuals have the right to request access to the personal information Akka holds about them. Akka responds to access requests within a reasonable timeframe and provides information in the format requested where practicable. Procedures for making access requests are described in Akka's Privacy Policy.

APP 13 — Correction of Personal Information

Individuals may request correction of personal information that is inaccurate, out-of-date, incomplete, irrelevant, or misleading. Akka's correction procedures are documented and accessible via the Privacy Policy and customer support channels. Where Akka declines to

correct, the individual is notified with reasons and informed of their right to complain to the OAIC.

Supporting Evidence

Akka's compliance with the Australian Privacy Principles is supported by the following evidence:

- Published Privacy Policy available at akka.io
- Data Processing Agreements with all significant sub-processors
- SOC 2 Type II reports from Amazon Web Services (infrastructure) and Google Cloud Platform (infrastructure)
- ISO 27001-aligned ISMS with documented privacy controls
- Employee privacy and security awareness training records
- Incident response plan and breach notification procedures
- Internal audit reviews conducted through Akka's annual ISMS audit cycle

Conclusion

Akka is fully compliant with the Australian Privacy Act 1988 and all 13 Australian Privacy Principles. All 15 controls in Akka's APP compliance programme are implemented, and the overall risk profile is Low. Akka's privacy programme is subject to annual review and continuous improvement within the ISMS.

This attestation is available to customers and prospects on request and may be shared under the terms of Akka's standard non-disclosure agreement.



Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Signed:

Michael Nash

Chief Information Security Officer

Akka Technologies, Inc.

michael.nash@akka.io

Date: 20 April 2026