AKKA

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

Singapore Personal Data Protection Act 2012 (PDPA) — Compliance Attestation

Introduction

This document constitutes Akka's formal attestation of compliance with the Singapore Personal Data Protection Act 2012 (PDPA), as amended by the Personal Data Protection (Amendment) Act 2020. It is intended for customers, prospects, and auditors seeking assurance about Akka's personal data handling practices as they relate to individuals whose personal data is governed by Singapore's PDPA.

This attestation is made by Akka's Chief Information Security Officer and reflects the state of Akka's PDPA compliance 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 processes personal data governed by Singapore's PDPA in the course of:

- Providing SaaS platform services to Singapore-based enterprise customers
- Processing account data, usage data, and support communications from Singapore individuals
- Acting as a data intermediary (processor) for personal data that Singapore customers process using the Akka platform

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

- Managing commercial relationships with Singapore partners and customers

The PDPA applies to Akka as an organisation collecting, using, or disclosing personal data of individuals in Singapore in connection with its business activities. Akka acts as both an organisation (controller) for its own customer relationship data and a data intermediary (processor) for data processed by customers through the Akka platform.

Compliance Posture

Akka has implemented a comprehensive PDPA compliance programme. As of the attestation date:

- Total controls: 9
- Controls Implemented: 9 (100%)
- Controls Not Applicable: 0
- Overall risk profile: All 9 controls rated Medium risk
- Compliance status: Compliant

Akka maintains an ISO 27001-aligned Information Security Management System (ISMS) that underpins its PDPA compliance programme. Privacy obligations are operationalised through documented policies, technical controls, and contractual mechanisms with customers and sub-processors.

Key Controls

AKKA

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

Consent Obligation

Akka obtains the consent of individuals before collecting, using, or disclosing their personal data, unless an exception under the PDPA applies. Consent is obtained through clear and explicit consent flows in Akka's SaaS platform and website. Individuals are informed of the purposes for collection at or before the time of collection. Consent records are maintained and auditable. Akka does not collect personal data beyond what is necessary for the notified purposes.

Purpose Limitation Obligation

Akka collects, uses, and discloses personal data only for purposes that a reasonable person would consider appropriate in the circumstances, and for which consent has been obtained. Where Akka wishes to use personal data for a new purpose, fresh consent is sought. Personal data is not repurposed without authorisation.

Notification Obligation

At or before the time of collection, Akka notifies individuals of the purposes for which their personal data is being collected, used, or disclosed. This notification is provided through Akka's Privacy Policy (available at akka.io) and through in-product disclosures. For enterprise customers processing data through the Akka platform, purposes are documented in Data Processing Agreements.

Accuracy Obligation

Akka takes reasonable steps to ensure that personal data collected is accurate and complete, particularly where the data may be used to make a decision that affects the individual or may be disclosed to a third party. Customers are provided with self-service tools to review and

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

correct their personal data, and Akka's support processes include procedures for handling correction requests promptly.

Protection Obligation

Akka implements security arrangements appropriate to the nature of the personal data held and the harm that could result from unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks. Security 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 annual penetration testing
- Security incident response procedures with defined escalation timelines
- Employee security awareness training

Akka's primary infrastructure is hosted on Amazon Web Services and Google Cloud Platform, both of which hold current SOC 2 Type II certifications.

Retention Limitation Obligation

Akka retains personal data only for as long as it is necessary to fulfil the purposes for which it was collected, or as required by law. Data retention schedules define maximum retention periods by data category. Automated and manual deletion processes enforce these limits. When personal data is no longer required, it is securely disposed of or anonymised.

AKKA

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

Transfer Limitation Obligation

Akka transfers personal data outside Singapore only to countries or territories that provide a standard of protection comparable to the PDPA, or where contractual protections equivalent to the PDPA are in place. Data Processing Agreements with all significant sub-processors incorporate PDPA-equivalent transfer protections. Akka's primary sub-processors (Amazon Web Services, Google Cloud Platform) are bound by contractual data protection commitments.

Access and Correction Obligation

Individuals have the right to request access to personal data that Akka holds about them and to request correction of inaccurate data. Akka provides a clear process for submitting access and correction requests, described in the Privacy Policy. Requests are responded to within a reasonable timeframe. Where access or correction is declined, individuals are informed with reasons.

Mandatory Breach Notification

Following the 2020 PDPA amendments, Akka is required to notify the Personal Data Protection Commission (PDPC) of data breaches that are likely to result in significant harm to affected individuals, within 3 calendar days of assessing that a notifiable breach has occurred. Where the breach is likely to result in significant harm to individuals, those individuals must also be notified as soon as practicable. Akka maintains a documented breach response procedure aligned with these timelines. Breach response procedures are tested as part of Akka's annual incident response exercise.

Supporting Evidence

Akka's compliance with Singapore's PDPA is supported by the following evidence:

AKKA

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

- Published Privacy Policy at akka.io incorporating PDPA notification requirements
- Data Processing Agreements with all significant sub-processors
- SOC 2 Type II reports from Amazon Web Services and Google Cloud Platform
- ISO 27001-aligned ISMS with documented PDPA controls
- Employee data protection awareness training records
- Personal data breach response procedure aligned with the 3-day PDPC notification requirement
- Data retention schedules and deletion procedures
- Internal audit reviews conducted through Akka's annual ISMS audit cycle

Conclusion

Akka is fully compliant with the Singapore Personal Data Protection Act 2012, as amended in 2020. All 9 controls in Akka's PDPA compliance programme are implemented and rated Medium risk. Akka's PDPA programme covers all core obligations including consent, purpose limitation, notification, accuracy, protection, retention limitation, transfer limitation, access and correction, and mandatory breach notification. The programme is subject to annual review 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.

Signed:

Michael Nash

AKKA

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

Chief Information Security Officer

Akka Technologies, Inc.

michael.nash@akka.io

Date: 20 April 2026