

Canada PIPEDA — Compliance Attestation

Introduction

This document constitutes Akka's formal attestation of compliance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5, including the Breach of Security Safeguards Regulations (SOR/2018-64). It is intended for customers, prospects, and auditors seeking assurance about Akka's personal information handling practices as they relate to individuals in Canada.

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

Note: Canada's proposed Consumer Privacy Protection Act (CPPA, part of Bill C-27) would replace PIPEDA with a more comprehensive framework. Bill C-27 has not yet received Royal Assent. Akka monitors its progress and is positioned to adapt its programme upon enactment.

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. PIPEDA applies to Akka's collection, use, and disclosure of personal information of Canadian individuals in the course of commercial activities, including:

- Providing SaaS platform services to Canadian enterprise customers

- Processing account data, usage data, and support communications from Canadian individuals
- Managing commercial relationships with Canadian partners and customers
- Operating its website and developer portals accessible to Canadian users

Akka applies PIPEDA across all provinces unless substantially similar provincial legislation applies (currently Alberta, British Columbia, and Quebec for private-sector privacy). For Quebec residents, Akka also monitors obligations under Law 25 (Act to modernize legislative provisions as regards the protection of personal information).

Compliance Posture

Akka has implemented a comprehensive PIPEDA compliance programme based on the 10 Fair Information Principles set out in Schedule 1 of PIPEDA. 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 provides the governance and operational foundation for PIPEDA compliance. A designated Privacy Management Programme is in place, overseen by Akka's Chief Information Security Officer in the role of Chief Privacy Officer.

Key Controls

Accountability — Privacy Management Programme

Akka has designated its Chief Information Security Officer (CISO) as the individual accountable for Akka's compliance with PIPEDA's Fair Information Principles. A Privacy Management Programme is in place covering policies, procedures, staff training, and contractual protections. Akka ensures that third-party processors who receive personal information on Akka's behalf provide comparable levels of protection through contractual obligations. The CISO is the point of contact for privacy inquiries and complaints from Canadian individuals.

Identifying Purposes and Consent

Akka identifies the purposes for collecting personal information before or at the time of collection, and obtains meaningful consent from individuals. Purposes are described in plain language in Akka's Privacy Policy (available at akka.io) and through in-product disclosures. For enterprise customers, purposes are documented in Data Processing Agreements. Consent is obtained at the time of collection and individuals may withdraw consent at any time, subject to legal or contractual restrictions, with reasonable notice to Akka.

Limiting Collection

Akka collects only the personal information necessary for the identified purposes. Collection by fair and lawful means is a core principle of Akka's data practices. Akka does not collect personal information indiscriminately and reviews collection activities to ensure they remain proportionate to the stated purposes.

Limiting Use, Disclosure, and Retention

Personal information collected by Akka is used or disclosed only for the purposes for which it was collected, or with the individual's consent, or as required by law. Akka does not sell personal information to third parties. Retention schedules define maximum periods for each category of personal information; when information is no longer required, it is securely destroyed, erased, or anonymised.

Accuracy and Safeguards

Akka takes reasonable steps to ensure that personal information is accurate, complete, and up-to-date for the purposes for which it is used. Self-service tools allow customers to review and correct their account data. Akka implements security safeguards appropriate to the sensitivity of the information, including:

- Encryption of personal information 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
- Documented incident response and breach notification procedures
- Employee privacy and security awareness training

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

Openness and Individual Access

Akka's Privacy Policy makes information about its personal information management practices readily available to individuals, including the type of personal information held, how it is used, and how to contact the Privacy Officer. Individuals have the right to request access to their personal information held by Akka and to challenge its accuracy. Access requests are processed within a reasonable timeframe and without excessive cost. Where access is refused, individuals are informed with reasons and advised of their right to complain to the Office of the Privacy Commissioner of Canada (OPC).

Breach Notification to the OPC

Under the Breach of Security Safeguards Regulations (2018), Akka is required to notify the Office of the Privacy Commissioner of Canada (OPC) and affected individuals when a breach of security safeguards involving personal information creates a real risk of significant harm (RROSH). Akka maintains a documented breach response procedure aligned with this standard. Notifications to the OPC are made as soon as feasible following the RROSH determination. Records of all breaches (including those not meeting the RROSH threshold) are maintained for a minimum of 24 months.

Supporting Evidence

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

- Published Privacy Policy at akka.io incorporating PIPEDA transparency requirements
- Designated Privacy Officer (CISO) with accountability for PIPEDA compliance
- 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 PIPEDA controls
- Employee privacy and security awareness training records

- Breach response procedure aligned with RROSH standard and OPC notification requirements
- Breach and security incident records maintained for 24-month minimum retention
- Internal audit reviews conducted through Akka's annual ISMS audit cycle

Conclusion

Akka is fully compliant with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). All 9 controls in Akka's PIPEDA compliance programme are implemented and rated Medium risk. Akka's programme encompasses all 10 Fair Information Principles: accountability, identifying purposes, consent, limiting collection, limiting use/disclosure/retention, accuracy, safeguards, openness, individual access, and challenging compliance. 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

Chief Information Security Officer / Chief Privacy Officer

Akka Technologies, Inc.

michael.nash@akka.io

Date: 20 April 2026