AKKA

Lightbend Inc, d.b.a Akka

Privacy Policy

May 29, 2025

Contents

Contents i
1.1 Introduction . . . 1
1.2 Scope . . . 1
1.3 Referenced Policies . . . 1
1.4 Policy . . . 1
1.4.1 Summary . . . 1
1.4.2 Categories Of Personal Information Collected . . . 1
1.4.3 No Spam Promise . . . 2
1.4.4 Who We Share Your Personal Data With . . . 2
1.4.5 Cookie Policy . . . 3
1.4.6 Security . . . 3
1.4.7 Purpose and Legal Basis for Processing . . . 3
1.4.8 Retention . . . 3
1.4.9 Effective Date and Updates . . . 3
1.4.10 Contact and Request . . . 3
1.5 Supported Frameworks . . . 3
1.5.1 EU And UK General Data Protection Regulation . . . 3
1.5.2 California Consumer Privacy Act . . . 4
1.5.3 Canada's Anti-Spam Legislation . . . 4
1.5.4 Commitment to Comply with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF . . . 4
1.5.5 Commitment to Comply with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF . . . 5
1.5.5.1 Binding Arbitration . . . 5
1.5.5.2 Investigatory and Enforcement Powers . . . 5
1.5.5.3 Onward Transfers . . . 5
1.6 Compliance . . . 5

Index 12

1.1. Introduction

In this policy, we describe in summary the personal information we collect and how we use it, share it, and protect it.

The details on how we handle your personal information are enumerated in the related policies.

1.2. Scope

This policy applies to all personally identifiable information (PII) collected by Akka, except for that information related to Employees, Contractors and Applicants, which are covered under their own policies.

1.3. Referenced Policies

1. Terms of Use
2. Personal Information Handling Policy

1.4. Policy

1.4.1. Summary

- Akka respects privacy on all its websites and services.
- We collect information from you including identifiers, customer records, usage data, professional affiliations, and build profiles.
- No spam promise; we only send you operational, security, and transaction-related emails (unless you opt-in to our newsletter).
- We share data with affiliated service providers and resellers and also if we have your consent or during corporate transactions.
- We use cookies for session info and visitor identification.
- We take strong measures to protect your data from unauthorized access.
- Data is retained as necessary for its collected purpose.
- We comply with international standards and privacy regulations.

Akka, Inc. is committed to respecting your privacy on all of our websites and the products and services offered on these websites.

In this policy, we describe the personal information we collect and how we use it, share it, and protect it.

1.4.2. Categories Of Personal Information Collected

We collect the following types of personal information:

- **Identifiers:** Includes direct identifiers, such as name, alias user ID, username, account number or unique personal identifier; email address, phone number, address and other contact information; IP address and other online identifiers.
- **Customer Records:** Includes personal information, such as name, account name, user ID, contact information, education and employment information, payment information that individuals provide to us in order to purchase or obtain our products and services.
- **Commercial Information:** Includes records of products or services purchased, obtained, or considered, or other purchasing or use histories or tendencies.
- **Audio, Video And Electronic Data:** Includes audio, electronic, visual, thermal, olfactory, or similar information such as photographs and images (e.g., that you provide us) and call recordings (e.g., of customer support calls).
- **Usage Data:** Includes browsing history, clickstream data, search history, access logs and other usage data and information regarding an individuals interaction with our websites, products, mobile apps and other services, and our marketing messages and online ads.
- **Professional:** Includes professional and employment-related information (such as current and former employer(s) and position(s), business contact information and professional memberships).

- **Education:** Information about an individuals educational history (such as the schools attended, degrees you were awarded, and associated dates).
- **Inferences:** Includes inferences drawn from other personal information that we collect to create a profile reflecting an individuals preferences, characteristics, predispositions, behavior, attitudes, abilities or aptitudes.
- **Information You Provide To Akka:** We collect personal data that you choose to provide to us when you are using our sites and services. Personal data may include your name, email address, state and country of residence, job title and company name. As part of the services, we may collect information about the courses you complete and any accreditations you receive. We may also collect personal data from your communications with us, including through email or forms on our sites, such as your phone number, and address. When engaging with our sales teams, we may collect your contact information, as well as information about your previous purchases and sales activity.
- **Information Automatically Collected:** Whenever you visit or interact with the sites, we automatically collect data about your visit. Such information includes your computer's Internet Protocol ("IP") address, device ID, device location information based on IP address, browser type, browser version, the pages you visit, the time and date of your visit, the time spent on those pages and other statistics.

1.4.3. No Spam Promise

We hate spam. You hate spam.

We dont send promotional messages or bulk email messages to you unless you have explicitly opted-in to our newsletter.

We crafted this policy to quell the frustration with spam and to better comply with US Federal Law, the CAN-SPAM Act of 2003, California State Law SB186, and Directives 2000/31/EC and 2002/58/EC of the European Parliament and of the Council, among others.

You will only receive email by an email address provided during a sign-up registration procedure or an email address provided voluntarily when filling out a newsletter or contact form.

We will contact you via email for business correspondence intended to inform customers of service, billing or business related issues. Also, to comply with several international information security standards including NIST CSF and the EU CRA, we are required to provide security and operational notifications to you.

Receipt emails or messages referring to transactions executed on our sites are NOT considered spam, since they are meant to confirm the status of a transaction for customers.

1.4.4. Who We Share Your Personal Data With

We do not share your personal data other than:

- **Affiliates, Service Providers And Processors:** We engage third party companies, individuals and affiliated entities to facilitate our sites and services and to provide the sites and services on our behalf, to perform related services, to assist us in analyzing how our sites and services are used, and to provide data storage and other services. These third parties have access to your personal data only to perform specific tasks on our behalf and are obligated to *not* retain, disclose, sell or use your personal data for any other purpose.
- **Resellers**: We engage third party value added service providers and their affiliates to facilitate execution of business transactions. These third parties have access to data collected about you and your entity only to perform specific tasks on our behalf are obligated to not retain, disclose, sell or use your personal data for any other purpose.
- **Third Parties In Case Of Legal Requirement:** We may share your personal data with third parties if we are legally required to do so. This includes situations where we need to comply with legal processes, assist law enforcement in investigating fraud or legal violations, respond to claims against us, or protect the rights, property, or safety of Akka, our customers, or the public.
- **Third Parties With Consent:** We will also disclose information about you, including personal data, to any other third parties, where you have expressly consented or requested that we do so.
- **Third Parties In Case Of A Corporate Transaction:** In addition, your personal data may be disclosed as part of any merger, sale, reorganization, transfer of Akka's assets or businesses, acquisition, bankruptcy, or similar event.

1.4.5. Cookie Policy

We use so-called Cookies and other similar technical means to track repeat visits to our sites and services in order to maintain session information, identify repeat visitors, and for other purposes relating to the delivery of our services.

See our Terms of Use for details.

1.4.6. Security

In order to protect your personal data we have implemented reasonable, commercially acceptable security procedures and practices appropriate to the nature of the personal data we store, in order to protect it from unauthorized access, destruction, use, modification or disclosure. Your personal data is contained behind secured networks and is only accessible by a limited number of people, who have special access rights and are required to keep the personal data confidential. Please see our Trust Center for information about our Information Security standards and policies. We require all third-parties with whom we share your data for processing to have equivalent security measures to our own.

1.4.7. Purpose and Legal Basis for Processing

We use personal information for various business purposes, including providing and improving our services, marketing, to provide customer support, and compliance with legal obligations.

1.4.8. Retention

We will retain your personal data for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

1.4.9. Effective Date and Updates

This policy is effective as of August 1st, 2024. We may update this policy from time-to-time, and you are welcome to subscribe on our Trust Center to be informed of such updates.

1.4.10. Contact and Request

We are Akka (Lightbend, Inc. d.b.a Akka), located at 580 California, #1231, San Francisco, CA 94104.

You can contact us via email at security@akka.io or by phone at 1 877 989-7372, or our website at https://www.akka.io to make requests about your personal information or any other privacy matters.

1.5. Supported Frameworks

Below is the required language for the privacy regulations and standards we comply with

1.5.1. EU And UK General Data Protection Regulation

Identity And Contact Details Of The Data Controller

Our Data Protection Officer for the EU can be reached at privacy_eu@akka.io.

Our Data Protection Officer for the UK can be reached at privacy_uk@akka.io.

For the UK, any complaints or for further information, you can contact the Information Commissioner's Office (ICO) in the UK at the ICO Official Website, the Helpline 0303 123 1113 or the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom.

You may find corresponding contact information for each of the EU member states at the European Data Protection Board Members Website

Description Of Data Subjects' Rights

You have the following rights regarding your personal data:

- The right to determine if we are holding any personal data relating to you (right to be informed).
- The right to access your data and request a copy (right of access).
- The right to rectify any inaccurate or incomplete data (right to rectification).
- The right to request the erasure of your data (right to erasure).
- The right to restrict the processing of your data.
- The right to data portability.
- The right to object to the processing of your data.

- The right to object to automated decision-making relating to your data, including profiling.
- The right to withdraw consent at any time.

Information On Data Transfers

Your data may be transferred to third countries outside the EU or UK. We ensure that appropriate safeguards are in place, such as standard contractual clauses, to protect your data.

Right To Lodge A Complaint

If you believe that your data protection rights have been violated, you have the right to lodge a complaint with the supervisory authority in your country (as listed above).

Automated Decision-Making And Profiling

We do not use automated decision-making or profiling that produces legal effects or that significantly affects you.

Source Of Data

If we have not collected data directly from you, we obtained it from publicly available sources. The categories of personal data we collect include those enumerated above. You must provide your content by explicit actions, either by registering on our website, or accepting a question asking for your consent to cookies and other such tracking, before we will collect data. You may withdraw such consent at any time by contacting us at privacy@akka.io, or using unsubscribe links in communications or on our website, which we will honor immediately.

1.5.2. California Consumer Privacy Act

Rights Under CCPA
You have the right to know what personal information we collect, use, disclose, and sell. You also have the right to request the deletion of your personal information, opt-out of the sale of your personal information, and not be discriminated against for exercising these rights.

Methods For Submitting Requests
You can submit requests to know or delete your personal information by contacting us as listed above in INTERNAL-CON.

Do Not Sell My Personal Information Link
If you wish to opt-out of the sale of your personal information, please email us at privacy@akka.io or use the Do Not Sell My Personal Information link on our website.

1.5.3. Canada's Anti-Spam Legislation

Consent For Communications
We obtain explicit consent before sending any commercial electronic messages. By subscribing to our newsletter or other services, you agree to receive promotional content from Akka. You can withdraw your consent at any time by using the unsubscribe link provided in our communications or by contacting us as detailed in INTERNAL-CON.

Unsubscribe Mechanism
To unsubscribe from our newsletter, click the unsubscribe link at the bottom of any of our messages. Your request will be processed immediately, and you will no longer receive newsletter emails from us.

1.5.4. Commitment to Comply with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF

Akka (Lightbend Inc, d.b.a "Akka") complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce.

Akka has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Akka has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF.

If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit https://www.dataprivacyframework.gov/

1.5.5. Commitment to Comply with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Akka commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioners Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

1.5.5.1 Binding Arbitration

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Akka is obligated to arbitrate claims and follow the terms set forth in Annex I of the DPF Principles, providing the individual making the claim has invoked binding arbitration by delivering notice to us and following the procedures and conditions set forth in Annex I of the Principles.

1.5.5.2 Investigatory and Enforcement Powers

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Akka is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC)

1.5.5.3 Onward Transfers

In the context of an onward transfer, Akka has responsibility for the processing of personal information it receives under the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF and subsequently transfers to a third party acting as an agent on its behalf.

Akka shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless we prove that we are not responsible for the event giving rise to the damage.

1.6. Compliance

For Akka employees, failure to comply with this policy may result in progressive discipline up to and including dismissal. For non-Akka employees and contractors, failure to comply may result in removal of the individual's ability to access and use Akka data and systems. Employers of non-Akka employees will be notified of any violations.

Glossary

ISO/IEC 27001 Information technology - Security techniques - Information security management systems. 6

ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management controls. 6

ISO/IEC 27005 Information technology - Security techniques - Information security risk management. 6

ISO/IEC 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and Guidelines. 6

Acceptable Risk Acceptable risk is the risk level that the management is prepared to accept as a business risk.. 6

ACL-DVS Assurance Life Cycle - Development Security. 6

AI Artificial Intelligence: Systems or applications that use machine learning algorithms, deep learning, natural language processing, or other techniques to perform tasks that typically require human intelligence.. 6

AI Risk Management Framework A structured approach to identifying, assessing, and mitigating risks associated with AI systems, as outlined by the NIST.. 6

AICPA American Institute of Certified Public Accountants. 6

Akka Data Any data stored on or originating from systems controlled by Akka for business purposes, including data that originates from Akka, Akka customers or data relating to Akka customers, excluding data classified as Public.. 6

Akka IT Members of Internal IT at Akka.. 6

ALC Assurance Life Cycle. 6

ALC-DES (Application Lifecycle) Delivery. 6

ALC-DLS (Application Lifecycle) Development Lifecycle. 6

ALC-DVS (Application Lifecycle) Development Security. 6

ALC-DVS.1.1.1C In the context of the EUCC (European Union Common Criteria) standard, ALC-DVS.1.1.1C is a specific assurance component within the Common Criteria framework. It falls under the ""ALC"" (Assurance Life Cycle) class, specifically the ""Development Security"" (DVS) family.. 6

ALC-DVS.2 A component of the Assurance Life Cycle (ALC) class within the Common Criteria (CC) framework (EUCC), specifically under the Development Security (DVS) family. This component requires that security measures in place during the development of the Target of Evaluation (TOE) are sufficient to protect the TOE and its associated assets. It aims to ensure that the development environment is secure and that the measures are adequate to maintain the confidentiality and integrity of the TOE throughout its development.. 6

Assets Entities that the owner of the TOE presumably places value upon. In the context of a Development Security System, assets are information in electronic or other form, information processing facilities and referring processes (incl. access control and alarm systems), development tools and environments, any manifestation of the TOE, and customer code and data provided to produce the TOE. 6

Assurance Classes Various assurance classes introduced and described in Part 3 of the Common Criteria.. 6

ATE Application Test. 6

Authentication Refers to the controls for providing Remote Users the means to verify or validate a claimed identity through the presentation of something they know (e.g., passwords), something they own (e.g., token), or something they are (e.g. fingerprint, biometrics, etc.).. 6

Authorization Refers to the controls for determining the resources that Remote Users are permitted to access based upon the permissions and privileges for which they have been authorized.. 6

Availability The property of being accessible and usable upon demand by an authorized entity. Business operations: General term for the entirety of operations performed by the developer related to the TOE, e.g. “personalization” is part of business operations.. 6

Business Continuity Planning Business Continuity Planning is concerned with keeping business operations running perhaps in another location or by using alternative tools and processes following a disaster.. 6

Business Impact Analysis Business Impact Analysis predicts the consequences of disruption of a business function, processes and gathers information needed to develop recovery strategies.. 6

C-SCRM Cybersecurity Supply Chain Risk Management. 6

can The word “can” is used for statements of possibility and capability, whether material, physical or causal. 6

CB Certification Body.. 6

CEM Common Evaluation Methodology.. 6

CFR Code of Federal Regulations (U.S.). 6

CISA The U.S. government’s Cybersecurity & Infrastructure Security Agency. 6

COBIT Control Objectives for Information and Related Technology. 6

Collector A business that buys, rents, gathers, obtains, receives, or accesses any personal information about a California resident by any means.. 6

Company Workstation A computing device owned by Akka and supplied to an Akka team member for use in performance of their job duties.. 6

Components A unit of software or hardware that can be both an entire system unto itself and used as part of a larger system. A component can be an entire operating system, a chip, an application, a package, a library, or even a single file or segment of source code. 6

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.. 6

confidentiality and/or integrity The expression “confidentiality and/or integrity” means either “confidentiality” or “integrity”, or a combination of both. 6

CONOPS Concept of Operations. 6

Consent Consent of the Data Subject means any freely given, specific, informed, and unambiguous indication of the Data Subject’s wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.. 6

Consumer A natural person who is a California resident (CCPA). 6

Control Set of measures, associated to one or more objectives, intended to respond to threats.. 6

Controller The natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.. 6

COTS Common off-the-shelf. 6

cPP Common Criteria Collaborative Protection Profile, or just Collaborative Protection Profile (see https://www.commoncrite
6

CREF Common Criteria for SOC 2 (CREF). 6

CRM Customer Relationship Management. 6

Cross-Border Transfers Transfers of personal data from and to different establishments of the controller or processor, all located within the EU, or transfers of personal data from data subjects are in the different EU Member States to the controller or processor establishment which is based in an EU Member State. 6

CSF The NIST Cyber Security Framework (v2.0). 6

CSIRT Computer Security Incident Response Team. 6

CUI Controlled Unclassified Information. 6

CVE Common Vulnerabilities and Exposures. 6

CVRF Common Vulnerability Reporting Format. 6

CVSS Common Vulnerability Scoring System. 6

CWE Common Weakness Enumeration. 6

Data processing facilities Premises, equipment, installation or tool used for data processing. 6

Data Processing Register A record of processing activities that includes significant information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients. 6

Data Subject Request A request made by an individual or an individual's legal representative to request Akka to do something which falls under one of the rights granted to EU-based individuals by the GDPR.. 6

Data Subjects An identified or identifiable natural person.. 6

Deployer Any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity. 6

Developer Entity (Site) offering services and being part of the development and production process; this encompasses all steps of the life cycle until delivery to the customer, e.g. software development, chip design, mask making, wafer production, testing, assembly etc. The developer is also responsible for supporting functions.. 6

Development environment Environment in which the TOE is developed; development includes the production of the TOE.. 6

Disaster Recovery Planning Disaster Recovery Planning is concerned with restoring normal business operations after a disaster takes place.. 6

DMZ Demilitarized Zone; in computer security, a DMZ is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.. 6

DORA The EU Digital Operational Resilience Act. 6

DSD Development Security Documentation (EU CRA). 6

DSS Development Security System (EU CRA). 6

DT Data Treatment: Refers to how data is collected, processed, stored, and managed within a system or organization. It encompasses the procedures and practices involved in handling personal and sensitive data.. 6

DVS Development Security. 6

Employment The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.. 6

ENISA Agence européenne chargée de la sécurité des réseaux et de l'information, the European Union Agency for Cybersecurity. 6

EU CRA European Union Cyber Resiliency Act: The goal of the CRA is to protect consumers and strengthen the EU's overall level of resilience. This means reducing the risks for all users of digital products, whether private individuals or public entities — corporations, hospitals, banks, utilities, postal services and so on. The CRA is mandatory, and compliance is required for CE marking of regulated products, as well as for distribution in the European market. The CRA includes some strict, coercive measures such as heavy fines.. 6

EU DORA The EU Digital Operational Resilience Act. 6

EUCC European Union Common Criteria, a standard for evaluating the security of information technology products and systems, ensuring they meet defined security requirements and specifications. The EUCC framework is derived from the SOG-IS Common Criteria which in turn is based on the ISO/IEC 15408-1 Common Criteria standard for Information Technology Security Evaluation. However, the SOG-IS adds an additional layer of mutual recognition among European countries. This means that a product evaluated and certified in one member state under SOG-IS is recognized by other member states, reducing the need for multiple evaluations.. 6

Facility Any equipment, installation or tool, regardless of being software or hardware, which is part of the security management system.. 6

FIPS Federal Information Processing Standards (U.S.). 6

FW Firmware. 6

GRC Governance, Risk, Compliance. 6

High Security Area Area where TOE related data or material classified “critical” or “very critical” is accessible, and Security Control areas (access control and intrusion detection) where applicable.. 6

High-Risk AI AI systems that have significant implications for individuals’ rights and freedoms, as defined under the EU AI Act.. 6

ICT Information and Communication Technology. 6

ICT Services Digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services. 6

ICT Third-Party Service Provider Any company (whether independent or part of a financial group) providing ICT services to financial entities. 6

IEC International Electrotechnical Commission, A global organization that prepares and publishes international standards for all electrical, electronic, and related technologies.. 6

Impact Impact (or consequence) refers to the extent to which a risk event might affect the organization.. 6

Incident An unplanned interruption or reduction in quality of service or breach of our Cloud Services SLA Policy, or any event that requires an immediate and time-sensitive response in order to avoid security or availability issues for our customers.. 6

Incident Bridge The means of live communication with anybody investigating the Incident. It will be ensured to be accessible by the Incident reporter, also.. 6

Incident Commander The person actively responsible for managing and resolving the Incident. They retain that role until an explicit hand off is made.. 6

Information Security Event Any occurrence related to information assets or the environment indicating a possible compromise of policies, failure of controls, or an unmapped situation that can impact security.. 6

Information Security Incident A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of information security policy.. 6

Inherent Risk The likelihood of an impact occurring when a threat compromises an unprotected asset. The current risk as it appears to the risk assessor before applying any control measures.. 6

Integrity The property of safeguarding the accuracy and completeness of assets.. 6

Intellectual Property Copyrights, trademarks, patents, and other information that is granted legal protections such as software.. 6

Internal Training Materials Media and content that you use to train your employees and partners.. 6

International data transfers Cross border flows of personal data from a Member State of the European Economic Area (the EU Member States and Liechtenstein, Iceland, and Norway) to a third country or international organization, as well as further transfers from that third country or organization to another country. 6

IP Intellectual Property (sometimes in technical context also Internet Protocol). 6

IS Information security - Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.. 6

IS event An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.. 6

IS Incident An Information Security (IS) incident. A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.. 6

ISMS Information Security Management System. 6

ISO International Organization for Standardization. It is an independent, non-governmental international organization that develops and publishes standards to ensure the quality, safety, efficiency, and interoperability of products, services, and systems. 6

ITIL Information Technology Infrastructure Library. 6

ITSEF ITSEF stands for Information Technology Security Evaluation Facility. It is an accredited laboratory responsible for conducting security evaluations of IT products and systems according to the Common Criteria standards. 6

JIL Joint Interpretation Library. 6

Likelihood How often the risk event might happen (e.g., per procedure/episode or within a specified timeframe).. 6

Malicious Code Virus, worms, Trojans, spyware and adware based on the perceived intent of the author.. 6

may Indicates a course of action permissible within the limits of the document. 6

Mobile Code Software obtained from remote systems transferred across the network, e.g. Java code, activeX controls, flash animations, office macros etc.. 6

NIST The U.S. National Institute of Standards and Technology, a U.S. federal government agency that develops technical standards, guidelines, and best practices in various fields, including cybersecurity, cryptography, and information technology as a part of the U.S. Department of Commerce. 6

OS Operating System. 6

OWASP Open Web Application Security Project. 6

Personal Device A device not owned by Akka, but owned by a User. Examples include personal cell phones, tablets, smart watches and so forth.. 6

Personal Information Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. (e.g., direct identifiers (real name, alias, postal address, social security numbers, driver's license, etc.), Indirect identifiers (cookies, IP addresses, account name, etc.), Biometric data, Internet activity, etc. See Personal Data.. 6

Remote Access Credentials Refers to identification and authentication credentials/data such as User IDs, passwords, tokens, etc.. 6

Remote Access Systems Refers to the systems, networks, and applications that facilitate remote access to Company information and systems.. 6

Sensitive Information Refers to information that is classified as other than Public.. 6

shall Indicates measures strictly to be followed in order to conform to the document and from which no deviation is permitted. 6

should Indicates that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. The CC interpret "not necessarily required" to mean that the choice of another possibility requires a justification of why the preferred option was not chosen. 6

TOE Target of Evaluation: Refers to the specific product, service, or system that is being assessed for cybersecurity compliance.. 6

Two-Factor Authentication Refers to the method of authentication that requires two factors before a Remote User will be allowed access to a network or system: a hardware or software token that produces a code that will change randomly at short time intervals and a password which is unique and only valid for the token.. 6

Vulnerability A weakness that could permit a threat to compromise the security of information assets.. 6

Index

California Consumer Privacy Act
INTERNAL 4
Canada's Anti-Spam Legislation
INTERNAL 4
Categories Of Personal Information Collected
INTERNAL 1
Commitment to Comply with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF
INTERNAL 4
Contact and Request
INTERNAL 3
Cookie Policy
INTERNAL 2

Effective Date and Updates
INTERNAL 3
EU And UK General Data Protection Regulation
INTERNAL 3

INTERNAL
California Consumer Privacy Act 4
Canada's Anti-Spam Legislation 4
Categories Of Personal Information Collected ... 1
Commitment to Comply with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF 4
Commitment to Comply with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF ..... Binding Arbitration5, Investigatory and Enforcement Powers5, Onward Transfers5
Contact and Request 3
Cookie Policy 2
Effective Date and Updates 3
EU And UK General Data Protection Regulation 3
No Spam Promise 2
Purpose and Legal Basis for Processing 3
Retention 3
Security 3
Summary 1
Who We Share Your Personal Data With 2

No Spam Promise
INTERNAL 2

PII 1
Policy
Privacy 1–3
Privacy 1
Policy 1–3
Supported Frameworks 3–5
Purpose and Legal Basis for Processing
INTERNAL 3

Retention
INTERNAL 3

Security
INTERNAL 3
Summary
INTERNAL 1
Supported Frameworks
Privacy 3–5

Who We Share Your Personal Data With
INTERNAL 2