AKKA

Lightbend Inc, d.b.a Akka

Privacy Policy

2026-04-13

Version 1

Contents

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. Referenced Frameworks and Standards

1. California Consumer Protection Act
2. Cloud Security Alliance Security, Trust and Assurance Registry
3. EU General Data Protection Regulation
4. India Digital Personal Data Protection Act 2023
5. Japan Act on the Protection of Personal Information (APPI)
6. Turkey Law on Protection of Personal Data (KVKK) No. 6698
7. UK General Data Protection Regulation
8. Akka's Internal Assurance Framework

1.5. Policy

1.5.1. 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.

1.5.2. 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 individual's 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 individual's 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 individual's 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.

1.5.3. No Spam Promise

We hate spam. You hate spam.

We don't 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.

1.5.4. 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.

1.5.5. 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.

1.5.6. 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.

1.5.7. 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.

1.5.8. 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.

1.5.9. 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.

1.5.10. 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.

1.5.11. AI Data Isolation in Production Environments

Where your data is hosted in a dedicated production environment, we do not process that data using any AI system — including systems operated by Akka or by our subcontractors and third-party tool providers — unless you have expressly opted in to such use in writing.

1.5.12. AI System Vetting for Customer Data

Akka shall not use any AI system in connection with customer confidential information unless:

1. the AI system has been approved and vetted to confirm it is technically configured to prevent customer data from being used to train, fine-tune, develop, or improve any underlying model or algorithm; and
2. the AI provider is bound by a written agreement prohibiting use of customer data for any purpose other than delivering services to Akka.

1.5.13. AI Features Are Opt-In

AI features and functionality are not enabled by default in your production environment. No AI feature or functionality is activated within your environment without your prior written consent, obtained through a specific opt-in process requiring your affirmative configuration. Our products and services do not incorporate AI as a standard or default feature.

1.6. Supported Frameworks

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

1.6.1. 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.

1.6.2. California Consumer Privacy Act

1.6.2.0.1 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.

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

1.6.2.0.3 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.

1.6.3. Canada's Anti-Spam Legislation

1.6.3.0.1 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.

1.6.3.0.2 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.

1.6.4. 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/

1.6.5. Complaints

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 Commissioner's 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.

1.6.5.1 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.

1.6.5.2 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)

1.6.5.3 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.

1.7. 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

EEA States The EU Member States as well as Iceland, Liechtenstein and Norway.. *see* EEA & EU

Agence nationale de la sécurité des systèmes dínformation The French National Agency for the Security of Information Systems. Agence nationale de la sécurité des systèmes dínformation is the National Cybersecurity Certification Authority for France and a leading authority in Common Criteria evaluation and EUCC certification.. *see* EUCC & National Cybersecurity Certification Authority

Bundesamt für Sicherheit in der Informationstechnik The German Federal Office for Information Security. The BSI is the National Cybersecurity Certification Authority for Germany and one of the most active national authorities in Common Criteria evaluation and EUCC certification in Europe.. *see* EUCC & National Cybersecurity Certification Authority

Centro Criptológico Nacional The Spanish National Cryptologic Centre. Centro Criptológico Nacional acts as the National Cybersecurity Certification Authority for Spain under the EUCC scheme and oversees Common Criteria evaluations performed in Spain.. *see* EUCC & National Cybersecurity Certification Authority

Comité français dáccréditation The French national accreditation body responsible for accrediting Conformity Assessment Bodys and other conformity assessment organisations in France, including those operating under EUCC.. *see* Conformity Assessment Body & EUCC

Conformity Assessment Body An accredited organisation authorised by the relevant National Cybersecurity Certification Authority to perform security evaluations and issue evaluation reports under a cybersecurity certification scheme such as EUCC.. *see* EUCC & National Cybersecurity Certification Authority

Development A CC assurance class (designator *ADV*) covering evidence about the design and implementation of the TOE, including functional specification, architectural design, and implementation representation.. *see* CC & TOE

Elliptic Curve Digital Signature Algorithm A digital signature algorithm based on elliptic curve cryptography. Elliptic Curve Digital Signature Algorithm provides equivalent security to Rivest–Shamir–Adleman with shorter key lengths and is widely used for TLS certificates and code signing.. *see* Rivest–Shamir–Adleman & TLS

European Cybersecurity Certification Framework The framework established by the EU Cybersecurity Act for creating European cybersecurity certification schemes. EUCC is the first scheme adopted under the European Cybersecurity Certification Framework.. *see* EUCC

Evaluation Assurance Level A numeric rating (EAL1–EAL7) assigned by a CC evaluation that indicates the depth and rigour of the security examination. Higher Evaluation Assurance Level values demand more comprehensive analysis and testing.. *see* CC

Evaluation Technical Report A confidential document produced by a Conformity Assessment Body summarising the evaluation evidence, methodology, and conclusions. Submitted to the National Cybersecurity Certification Authority as the basis for issuing a CC certificate.. *see* Conformity Assessment Body, CC & National Cybersecurity Certification Authority

Guidance Documents A CC assurance class (designator *AGD*) covering evaluation of the operational and preparative guidance provided to administrators and users of the TOE.. *see* CC & TOE

Impact Analysis Report A document produced during maintenance of a CC certificate that assesses whether a change to the certified TOE affects the validity of the existing certificate and determines what re-evaluation, if any, is required.. *see* CC & TOE

National Competent Authority A national authority within an EU member state designated to oversee cybersecurity matters. In the context of EUCC, the National Competent Authority may also serve as the National Cybersecurity Certification Authority.. *see* EUCC & National Cybersecurity Certification Authority

National Cybersecurity Certification Authority The national body designated under the EU Cybersecurity Act (Regulation (EU) 2019/881) to supervise cybersecurity certification activities and issue certificates under schemes such as EUCC within a member state.. *see* EUCC

Netherlands National Communications Security Agency The Dutch national authority for communications security, responsible for Common Criteria evaluation oversight and EUCC certification activities in the Netherlands.. *see* EUCC

Organismo di Certificazione della Sicurezza Informatica The Italian Certification Body for Information Security. **O**rganismo di **C**ertificazione della **S**icurezza **I**nformatica acts as the **N**ational **C**ybersecurity **C**ertification **A**uthority for Italy under the EUCC scheme.. *see* EUCC & **N**ational **C**ybersecurity **C**ertification **A**uthority

Protection Profile An implementation-independent set of CC security requirements for a category of product, used as a reusable baseline. Vendors may claim **P**rotection **P**rofile compliance within their **S**ecurity **T**arget.. *see* CC & **S**ecurity **T**arget

Secure Hash Algorithm A family of cryptographic hash functions standardised by NIST. SHA-256 and SHA-384 (from the SHA-2 family) and SHA-3 variants are approved for use in Akka systems; MD5 and SHA-1 are deprecated.. *see* NIST

Security Assurance Requirement A requirement drawn from CC Part 3 that specifies what the developer and evaluator must produce to demonstrate a given level of assurance. **S**ecurity **A**ssurance **R**equirements are composed into **E**valuation **A**ssurance **L**evels.. *see* CC & **E**valuation **A**ssurance **L**evel

Security Functional Requirement A requirement drawn from CC Part 2 that specifies the intended security behaviour of the TOE. **S**ecurity **F**unctional **R**equirements are stated in the **S**ecurity **T**arget and verified during the evaluation.. *see* CC, **S**ecurity **T**arget & TOE

Security Problem Definition The section of a **S**ecurity **T**arget or **P**rotection **P**rofile that formally describes the threats, organisational security policies, and assumptions that the TOE is designed to address.. *see* **P**rotection **P**rofile, **S**ecurity **T**arget & TOE

Security Target A document defining the security problem, objectives, and summary of security specifications for a specific TOE. The **S**ecurity **T**arget is the primary artefact evaluated and certified under CC.. *see* CC & TOE

TOE Summary Specification A section of the **S**ecurity **T**arget that describes how the TOE satisfies each of its **S**ecurity **F**unctional **R**equirements, bridging the security requirements and the implemented product.. *see* **S**ecurity **F**unctional **R**equirement, **S**ecurity **T**arget & TOE

United Kingdom Accreditation Service The sole national accreditation body for the United Kingdom, responsible for accrediting **C**onformity **A**ssessment **B**odys and other conformity assessment organisations. Relevant to EUCC evaluations conducted by UK-based **C**onformity **A**ssessment **B**odys under mutual recognition arrangements.. *see* **C**onformity **A**ssessment **B**ody & EUCC

Vulnerability Assessment A CC assurance class (designator *AVA*) covering evaluation of the resistance of the TOE to exploitation by an attacker with defined attack potential.. *see* CC & TOE

AAO Akka Automated Operations - a managed platform deployed within a customer VPC that fully automates and supports production-grade, self-clustering and elastic agentic services built with the Akka SDK.. *see* Akka SDK & VPC

AI **A**rtificial **I**ntelligence - A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.. 4

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

AIMS **AI** **M**anagement **S**ystem – a management system for establishing, implementing, maintaining, and continually improving the governance of AI within an organization, as defined by ISO/IEC 42001.. *see* AI

Akka Application An application that is built using the Akka SDK. Akka applications contain APIs, workflows, streaming consumers, timers, and views for querying data. They are packed into Docker images and deployed as microservice instances within an Akka operating environment. Akka applications act as their own in-memory, durable database. They take responsibility for persisting their own state. Akka apps also cluster from within, creating a runtime cluster with other instances that handle balancing traffic, sharding data, and replicating their data to instances running within another region. Akka applications can be replicated between regions in different Akka Application Planes if needed.. *see* Akka Application Plane, Akka SDK & API

Akka Application Plane The runtime environment for hosting Akka applications within one or more regions. The Akka application plane provides compute, storage, and I/O to execute Akka apps. It also provides automation to increase or decrease application instance capacity, observability for monitoring and debugging application behavior, and infrastructure management. The application plane is responsible for ensuring an Akka application meets its SLA by managing the Akka application and the underlying infrastructure. Data in this plane does not leave your VPC nor does it interact with our Akka Federation Plane.. *see* Akka Federation Plane, SLA & VPC

Akka CLI The CLI for developers, operators, and InfoSec teams to interface with various Akka environments. The Akka CLI provides utilities for building, testing, packing, and deploying Akka applications. It also provides utilities for observability, secrets management, service scaling, and account management.. *see* CLI

Akka SDK SDK with support for programming components, a local debugging console, and a test kit for building, testing, and packing Akka applications.. *see* SDK

ALC-DVS.1.1.1C In the context of the EUCC standard, ALC-DVS.1.1.1C is a specific assurance component within the Common Criteria framework. It falls under the ALC class, specifically the DVS family.. *see* ALC, DVS & EUCC

ALC-DVS.2 A component of the ALC class within the CC framework (EUCC), specifically under the DVS family. This component requires that security measures in place during the development of the 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.. *see* ALC, CC, DVS, EUCC & TOE

ANPD **A**utoridade **N**acional de **P**roteção de **D**ados – the Brazilian National Data Protection Authority responsible for enforcing and overseeing compliance with the LGPD.. *see* LGPD

AOC **A**ttestation of **C**ompliance – A formal self-assessment document or report completed by a merchant or service provider to certify compliance with the PCI-DSS, confirming that all applicable requirements have been met.. *see* PCI-DSS

ARN **A**mazon **R**esource **N**ame - A unique identifier for AWS resources used in IAM policies, service configurations, and audit logs to unambiguously reference any resource across the AWS platform.. *see* AWS & IAM

Assets Entities that the owner of the TOE presumably places value upon. In the context of a DSS, 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. *see* DSS & TOE

Authentic Data In the context of the EU DORA, data from a statutory public register, the dissemination and/or processing of which is subject to statutory requirements and which are disclosed by the customer to third parties in connection with the performance of a contract.. *see* EU DORA

BAA **B**usiness **A**ssociate **A**greement - A contract required under HIPAA between a Covered Entity and a Business Associate that receives, creates, or transmits protected health information on its behalf, establishing each party's obligations for safeguarding that information.. *see* HIPAA

BCR **B**inding **C**orporate **R**ules - An approved data protection policy, under Article 47 of the GDPR, that allows multinational organisations to transfer personal data within their corporate group to entities in countries outside the EEA that do not provide an adequate level of protection.. *see* EEA & GDPR

BIA **B**usiness **I**mpact **A**nalysis – A structured process for identifying critical business functions and processes, quantifying the potential consequences of their disruption, and determining recovery priorities and objectives. See Business Impact Analysis.. *see* Business Impact Analysis

BSI Group **B**ritish **S**tandards **I**nstitution Group – A leading global standards body and certification authority that issues ISO/IEC 27001 and other management system certifications.. *see* IEC & ISO

Business Continuity Planning See Business Continuity Planning. *see* Business Continuity Planning

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.. *see* TOE

BYOD Abbreviation for **B**ring **Y**our **O**wn **D**evice, a corporate IT policy that permits employees to use their personal smartphones, laptops, or tablets to access company data and perform work tasks rather than relying on employer-provided hardware. See personal-device.. *see* IT

CCM **C**loud **C**ontrols **M**atrix – a cybersecurity control framework developed by the CSA that provides security controls mapped to leading industry standards for cloud environments.. *see* CSA

CD **C**ontinuous **D**eployment - The automated release of software builds that have passed all automated quality and security gates to production or a staging environment, typically as the final stage of a CI/CD pipeline.. *see* CI

CLD Cloud-specific control prefix used in ISO/IEC 27017 to designate controls applicable specifically to cloud service customers and providers (e.g., CLD.12.4.1 for monitoring of cloud services).. *see* IEC & ISO

CNAPP **C**loud-**N**ative **A**pplication **P**rotection **P**latform – An integrated security platform that combines CSPM, workload protection, and software composition analysis capabilities to secure cloud-native applications from development through runtime.. *see* CSPM

Confidence In Akka's ISMS, the confidence level assigned to a control following an internal audit, reflecting whether evidence was found that the Implementation Details are being followed in practice. Rated High, Medium, or Low.. *see* ISMS

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.. *see* Data Subject

Consumer In the context of the CCPA, A natural person who is a California resident.. *see* CCPA

CPA **C**ertified **P**ublic **A**ccountant - A licensed accounting professional qualified to perform independent audits; CPA firms conduct SOC 2 Type II attestation audits of service organisation controls.. *see* SOC

Critical or Important Function In the context of the EU DORA, a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.. *see* EU DORA

CSA **C**loud **S**ecurity **A**lliance – a non-profit organisation that promotes best practices for secure cloud computing and publishes guidance and frameworks including the CCM and the STAR certification programme.. *see* CCM & STAR

CSF The NIST Cyber Security Framework (v2.0). *see* NIST

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.. *see* EU & GDPR

Data Subjects See Data Subject.. *see* Data Subject

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. *see* AI

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

DORA The EU Digital Operational Resilience Act, or DORA Regulation. *see* DORA Regulation & EU

DORA CO DORA **C**ontractural **O**bligations - specific contractural obligations required to be in place by the EU DORA for regulated industries and their ICT suppliers.. *see* DORA, EU DORA & ICT

DR **D**isaster **R**ecovery is a set of policies, tools, and procedures used to regain access and functionality to IT infrastructure following a catastrophic event. While HA focuses on surviving small hardware failures, DR is the "Plan B" for major disasterssuch as fires, floods, cyberattacks (like ransomware), or massive regional power outages.. *see* HA & IT

DRP **D**isaster **R**ecovery **P**lan – a documented set of procedures to recover and restore IT systems, data, and operations following a disruptive event.. *see* IT

DSAR **D**ata **S**ubject **A**ccess **R**equest - A request by an individual under data protection law (e.g. GDPR) to obtain a copy of the personal data an organisation holds about them, along with information about how it is processed.. *see* GDPR

DSD Development Security Documentation, in the context of the EU CRA. *see* EU CRA

DSS Development Security System, in the context of the EU CRA. *see* EU CRA

EBA **E**uropean **B**anking **A**uthority – the EU regulatory body responsible for maintaining financial stability and ensuring the integrity of the European banking sector through binding technical standards and guidelines.. *see* EU

EBS **E**lastic **B**lock **S**tore - An AWS block storage service providing persistent, high-performance storage volumes for use with EC2 instances, supporting encryption at rest and point-in-time snapshots.. *see* AWS & EC2

EC2 **E**lastic **C**ompute **C**loud - An AWS service providing scalable virtual machine capacity in the cloud, used to run application workloads, container nodes, and managed services.. *see* AWS

ECS Amazon **E**lastic **C**ontainer **S**ervice – an AWS managed container orchestration service for deploying, managing, and scaling containerized applications.. *see* AWS

EIOPA **E**uropean **I**nsurance and **O**ccupational **P**ensions **A**uthority – One of the three EU financial supervisory authorities responsible for regulating and supervising the insurance and occupational pension sectors, and jointly overseeing the designation of critical ICT third-party service providers under DORA.. *see* DORA, EU & ICT

EKS Amazon's **E**lastic **K**ubernetes **S**ervice - A managed service that automates the deployment, scaling, and management of **K**ubernetes control planes and infrastructure on AWS.. *see* AWS

ESMA **E**uropean **S**ecurities and **M**arkets **A**uthority – One of the three EU financial supervisory authorities responsible for regulating and supervising securities markets, and jointly overseeing the designation of critical ICT third-party service providers under DORA.. *see* DORA, EU & ICT

EU CRA EU **C**yber **R**esiliency **A**ct: 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.. *see* CE Marking & EU

EU DORA See DORA. *see* DORA

EU GDPR Specifically the EU version of the GDPR.. *see* EU & GDPR

EUCC **E**uropean **U**nion **C**ommon **C**riteria, 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.. *see* IEC & ISO

GPG **G**NU **P**rivacy **G**uard - A free, open-source implementation of the OpenPGP standard for encrypting and digitally signing data, widely used for signing software release artefacts and verifying their integrity.. *see* OpenPGP

gRPC gRPC - An open-source remote procedure call framework using HTTP/2 transport and Protocol Buffers serialisation, enabling efficient, strongly typed, language-agnostic communication between services.. *see* HTTP

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.. *see* TOE

ICT Asset In the context of the EU DORA, a software or hardware asset in the network and information systems used by the financial entity.. *see* EU DORA

ICT Risk In the context of the EU DORA, any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.. *see* EU DORA

ICT Services In the context of the EU DORA, 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.. *see* EU DORA & ICT

ICT Third-Party Risk An ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements.. *see* ICT

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

ICT-Related Incident In the context of the EU DORA, a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity.. *see* EU DORA

ICTS **I**nformation and **C**ommunication **T**echnology **S**ecurity – The practice of protecting ICT systems, networks, and data from threats, ensuring the confidentiality, integrity, resilience, and availability of digital infrastructure.. *see* ICT

IS Incident An 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.. *see* IS

ISO/IEC 27701 Security techniques Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management Requirements and Guidelines. *see* IEC & ISO

ITSEF **I**nformation **T**echnology **S**ecurity **E**valuation **F**acility. It is an accredited laboratory responsible for conducting security evaluations of IT products and systems according to the Common Criteria standards. *see* IT

LLM **L**arge **L**anguage **M**odel – a type of AI model trained on large text corpora and capable of generating, summarising, translating, and reasoning about natural language.. *see* AI

Major ICT-Related Incident In the context of the EU DORA, an ICT-Related Incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity.. *see* EU DORA & ICT-Related Incident

MGF **M**odel **G**overnance **F**ramework – Singapore's regulatory framework, published by the Monetary Authority of Singapore, for governing the responsible development and deployment of AI models in financial services.. *see* AI

ML **M**achine **L**earning – a branch of AI in which systems learn from data to improve performance on tasks without being explicitly programmed for each case.. *see* AI

NACL **N**etwork **A**ccess **C**ontrol **L**ist - A stateless firewall rule set in AWS that controls inbound and outbound traffic at the subnet level within a VPC, evaluated in rule-number order.. *see* AWS & VPC

Nasjonal sikkerhetsmyndighet The Norwegian National Security Authority, responsible for supervising protective security in Norway and acting as the national authority for Common Criteria evaluation and EUCC certification activities.. *see* EUCC

Network and Information System In the context of the EU DORA, An electronic communications network as defined in Article 2(1) of Directive (EU) 2018/1972; Any device or group of devices connected or associated with each other, one or more of which carry out automated processing of digital data based on a programme; or Digital data stored, processed, retrieved or transmitted by the elements specified for the purpose of their operation, use, protection and maintenance.. *see* EU DORA

NIS2 **N**etwork and **I**nformation **S**ystems Directive 2 – the EU cybersecurity directive (2022/2555) that strengthens security requirements and incident reporting obligations, extending scope to additional critical sectors compared to its predecessor.. *see* EU

NVD **N**ational **V**ulnerability **D**atabase - The US NIST repository of vulnerability management data, providing CVSS scores, remediation guidance, and searchable CVE records used to assess and prioritise security vulnerabilities.. *see* CVE, CVSS & NIST

OPC **O**ffice of the **P**rivacy **C**ommissioner – the Canadian federal authority responsible for overseeing compliance with PIPEDA and other federal privacy laws and promoting privacy rights.. *see* PIPEDA

P90 A statistical measure used to describe the performance of a system (usually latency or response time). If an SLA specifies a P90 of 500ms, it means that 90 percent of all requests are completed in 500ms or less.. *see* SLA

PDPA Singapore's **P**ersonal **D**ata **P**rotection **A**ct – Singapore's primary data protection legislation, enacted in 2012 and administered by the PDPC, governing the collection, use, and disclosure of personal data.. *see* PDPC

PEM Security of Critical Infrastructure Act 2018 (Cth) — Australian legislation that imposes risk management and mandatory incident notification obligations on owners and operators of critical infrastructure assets, including a 12-hour notification window to the ASD for critical cyber security incidents.. *see* ASD

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

PHD **A**WS **P**ersonal **H**ealth **D**ashboard - An AWS service providing personalised, real-time information about the health of AWS services and resources, including scheduled maintenance events and security notifications relevant to an account.. *see* AWS

PII **P**ersonally **I**dentifiable **I**nformation is any data that can be used on its own or with other relevant information to identify, contact, or locate a single person. See Personal Information.. *see* Personal Information

PIMS **P**rivacy **I**nformation **M**anagement **S**ystem — A management system for establishing, implementing, maintaining, and continually improving an organisationś privacy governance framework, built as an extension to an ISMS in accordance with ISO/IEC 27701.. *see* ISMS & ISO/IEC 27701

Privileged Users In the context of the EU DORA, Privileged users: system administrators and operators who supervise the operation of the system as a whole. In addition, there may also be users with privileged user rights or user rights with advanced functionality in a specific IT system (e.g. they may grant users read/write permissions).. *see* EU DORA

RDS **R**elational **D**atabase **S**ervice - An AWS managed database service supporting multiple relational database engines (including PostgreSQL, MySQL, and Aurora), providing automated backups, encryption at rest, and high availability.. *see* AWS

REST **R**epresentational **S**tate **T**ransfer - An architectural style for distributed hypermedia systems in which clients interact with server resources using standard HTTP methods; the dominant paradigm for designing web APIs.. *see* API & HTTP

RoPA **R**ecord **o**f **P**rocessing **A**ctivities - A mandatory documentation requirement under Article 30 of the GDPR that organisations must maintain, listing all personal data processing activities, their purposes, data categories, retention periods, and technical/organisational safeguards.. *see* GDPR

RoPA **R**ecord **o**f **P**rocessing **A**ctivities - A mandatory documentation requirement under Article 30 of the GDPR that organisations must maintain, listing all personal data processing activities, their purposes, data categories, retention periods, and technical/organisational safeguards.. *see* GDPR

S3 **S**imple **S**torage **S**ervice - An AWS object storage service providing high durability, scalability, and availability for storing and retrieving data, supporting encryption at rest, versioning, and access control policies.. *see* AWS

SAML **S**ecurity **A**ssertion **M**arkup **L**anguage - An XML-based open standard for exchanging authentication and authorisation data between identity providers and service providers, enabling SSO for enterprise applications.. *see* SSO

SCC **S**tandard **C**ontractual **C**lauses - Pre-approved contractual clauses issued by the European Commission that provide a legal mechanism for transferring personal data from the EEA to third countries that have not been deemed to offer an adequate level of data protection.. *see* EEA

SCC **S**tandard **C**ontractual **C**lauses - Pre-approved contractual clauses issued by the European Commission that provide a legal mechanism for transferring personal data from the EEA to third countries that have not been deemed to offer an adequate level of data protection.. *see* EEA

SCP **S**ervice **C**ontrol **P**olicy - An AWS Organizations policy type that defines the maximum set of permissions available to accounts within an organisational unit, used to enforce preventive governance guardrails across the entire AWS account hierarchy.. *see* AWS

SD **S**ecurity **D**omain - A classification framework for AI agent deployments that defines the security boundary across four dimensions: data classification, action scope, system boundary, and autonomy level; SD-1 denotes the first and most restrictive tier of this classification.. *see* AI

Significant Cyber Threat In the context of the EU DORA, a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-Related Incident or a major operational or security payment-related incident.. *see* EU DORA & ICT-Related Incident

SLO A **S**ervice **L**evel **O**bjective is a specific target or goal within an SLA. It is the technical benchmark that the team aims to hit to keep the customer happy. SLOs are usually more stringent than the SLA to provide a "safety buffer.". *see* SLA

SoA **S**tatement of **A**pplicability – a document required by ISO/IEC 27001 that lists all controls from Annex A, declares whether each is applicable to the organisation, and provides justification for any exclusions.. *see* ISO/IEC 27001

SOCI Act Security of Critical Infrastructure Act 2018 (Cth) — Australian legislation that imposes risk management and mandatory incident notification obligations on owners and operators of critical infrastructure assets, including a 12-hour notification window to the ASD for critical cyber security incidents.. *see* ASD

SPDX **S**oftware **P**ackage **D**ata **E**xchange - An open ISO/IEC standard (ISO/IEC 5962) for communicating SBOM information, including package identities, versions, license obligations, and provenance data.. *see* IEC, ISO & SBOM

SRE **S**ite **R**eliability **E**ngineering – a discipline that applies software engineering practices to IT operations, focusing on building reliable, scalable, and efficient systems through automation and measured service-level objectives.. *see* IT

STAR **S**ecurity, **T**rust, **A**ssurance and **R**isk – the CSA certification and registry programme that documents the security controls of cloud service providers, enabling customers to assess provider compliance.. *see* CSA

STS AWS **S**ecurity **T**oken **S**ervice – an AWS service that issues temporary, limited-privilege credentials for accessing AWS resources, supporting federated identity, cross-account access, and role assumption.. *see* AWS

Third Country In the context of the EU and EU customers, any State that is not a member of the EEA.. *see* EEA & EU

Threat-Led Penetration Testing In the context of the EU DORA, a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems.. *see* EU DORA

TIA **T**ransfer **I**mpact **A**ssessment - An assessment required when transferring personal data to a third country, evaluating whether the law and practice of the destination country ensures adequate protection for the data transferred in light of Article 46 of the GDPR.. *see* GDPR

Trade Secret In the context of the EU DORA, a fact, information, other data or an assembly thereof, connected to an economic activity, which is secret in the sense that it is not, as a body or as the assembly of its components, generally known or readily accessible to persons dealing with the affected economic activity and therefore it has pecuniary value, and which is subject to steps made with the care that is generally expected under the given circumstances, by the person lawfully in control of the information, to keep it secret. Protected knowledge (know-how), technical, economic or organisational knowledge, solution, experience or the assembly thereof that are classified as trade secret and recorded in an identifiable manner also constitute trade secrets.. *see* EU DORA

TSC The **T**rust **S**ervices **C**riteria are a set of control criteria developed by the AICPA to evaluate and report on the suitability of the design and operating effectiveness of controls at a service organization relevant to the Security (the only required criterion), Availability, Processing Integrity, Confidentiality, or Privacy of the information and systems used to process user data.. *see* AICPA

UK **U**nited **K**ingdom - The sovereign state comprising England, Scotland, Wales, and Northern Ireland. Following its departure from the EU, the UK maintains its own data protection regime under the UK GDPR and the Data Protection Act 2018.. *see* EU & GDPR

Index