



Lightbend Inc, d.b.a Akka

# Akka Availability Guarantee Policy

2026-04-13

Version 1

# Contents

<b>Contents</b>	<b>i</b>
1.1 Introduction . . . . .	1
1.2 Scope . . . . .	1
1.3 Referenced Policies . . . . .	1
1.4 Referenced Frameworks and Standards . . . . .	1
1.5 Availability Guarantee . . . . .	1
1.5.1 Guarantee . . . . .	1
1.5.2 Product Exclusions . . . . .	1
1.6 Availability Guarantee Claims . . . . .	2
1.6.1 Filing a Claim . . . . .	2
1.6.2 Validation . . . . .	2
1.6.3 Limitations and Application of Credits . . . . .	2
1.6.4 Issue Exclusions . . . . .	2
1.7 Compliance . . . . .	3
Glossary . . . . .	4
<b>Index</b>	<b>8</b>

## 1.1. Introduction

Akka believes in the resilience and reliability of its Software, to the point where Akka guarantees it to the extent described in this Policy.

Akka will guarantee a **99.9999%** availability of **your-application-services** that Customer builds with Akka and deploys into an Akka Region.

If Akka causes a loss of availability in [Your Application Services](#), Akka will reimburse Customer for the unavailability period in accordance with the terms and conditions set forth below.

## 1.2. Scope

This policy applies to [Your Application Services](#) that are deployed in more than one Akka Region and have [HA/DR](#) services activated by Customer for replication.

This guarantee does not apply to [Akka Federated Plane](#) (see the [Akka Federated Plane SLA](#) Policy) or other hosted services available at Akka.io;

## 1.3. Referenced Policies

1. [Resilience Guarantee Policy](#) - Akka's policy that guarantees Your Applications will never experience a data loss caused by Akka.
2. [Customer Support Policy](#) - Akka's policy that governs Akka's support and managed services SLA.

## 1.4. Referenced Frameworks and Standards

1. Akka's Internal Assurance Framework

## 1.5. Availability Guarantee

### 1.5.1. Guarantee

For [Your Application Services](#) deployed to more than one Akka Regions, Akka offers an availability (i.e., the ability of Your Application Services to respond to normal requests) guarantee of 99.9999% if the following conditions are met:

1. [Your Application Services](#) are deployed in an Akka Region configured using Akka's Tooling.
2. [Your Application Services](#) are deployed into at least two Akka Regions, with replication active along with [HA/DR](#) configured.
3. [Your Application Services](#) and the Akka Regions are accessible by Akka for monitoring purposes and for Akka to make configuration updates directly.
4. After each Major Change as determined by Customer, Customer will perform a performance and load test of [Your Application Services](#). [Your Application Services](#) must pass, as determined by Customer, such performance and load test. Minor changes and patches do not require performance and load test.

### 1.5.2. Product Exclusions

This guarantee does not apply to:

1. The [Akka Federation Plane](#) or other hosted services available at Akka.io (see the Cloud Services [SLA](#) Policy).
2. Self-Managed or other forms of deployment of any Akka product other than [AAO](#) in [BYOC](#) deployments.

## 1.6. Availability Guarantee Claims

### 1.6.1. Filing a Claim

Assuming Customer qualifies, to file a claim, Customer must open a support ticket via the [Support Portal](#) within seventy-two (72) hours of [Your Application Services](#) first exhibiting signs of non-availability behavior. The ticket should include:

- The unavailability time frame of [Your Application Services](#), and
- Either debug logs showing the unavailability events, or, a minimal reproducer that demonstrates the issue.

For the sake of clarity, this seventy-two (72) hour support ticket is to log an indication of system-wide non-availability for obtaining credits against this availability guarantee. If [Your Application Services](#) exhibit unplanned, multi-region non-availability, that scenario should be considered a Severity 1 issue with Customer opening the related support ticket immediately upon first knowledge thereof.

### 1.6.2. Validation

Customer's claim will be approved for remuneration only after Akka verifies that the issue that caused the downtime originated from issues caused by Akka.

Akka will attempt to validate the issue independently, however, Akka may require Customer's participation in order to diagnose the issue, including attempting suggested resolutions on a test system.

### 1.6.3. Limitations and Application of Credits

Once a claim is filed and validated, a reimbursement credit for ten (10) times the applicable fees (for annual subscriptions, the pro-rata allocation of Customer's total annual Software and managed services spend) of the non-available period will be issued.

This credit will be applied to Customer's future license or subscription (as applicable) fees with Akka and cannot be redeemed for cash or cash equivalent.

### 1.6.4. Issue Exclusions

This guarantee does not apply to issues:

1. Caused by factors outside of Akka's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Akka;
2. That result from any actions or inactions of Customer, including failure to acknowledge a recovery volume, initiate a failover, or respond to resource health concerns;
3. That result from issues that could have been prevented by executing a performance and load test prior to introducing a change into the environment.
4. That result from equipment, software or other technology not supplied by Akka, which includes unintended interference from Java Virtual Machine observability agents;
5. That result from Customer-scheduled downtime, maintenance, or upgrade windows;
6. That use a version of Akka's product where the root cause of the loss was caused by a known issue that has been resolved in a subsequent version;
7. That result from use of any pre-release of Software such as [Beta Release](#) or [Milestone Releases](#), except for Developer Support and agreed to by Akka in an applicable Order Form; or
8. That result from use of software not obtained from Akka under the Agreement.

## 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](#)

**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](#).. [1](#), *see* [Akka SDK](#) & [VPC](#)

**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](#)

**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 Federated Plane** The Akka Federated Plane is an online service to coordinate between Akka regions, providing maintenance and administrative operations to and between such regions.. [1](#)

**Akka Federation Plane** A global coordination point that is responsible for organizations, accounts, billing, and federating multiple Akka regions into a single substrate for which Akka applications can be deployed into. The Akka Federation Plane runs at Akka.io and is managed by Akka. The Akka Federation Plane is necessary for the deployment of Akka applications, while the application plane is responsible for your application's elasticity, availability, and resilience. An unavailable Federation Plane will not impact running Akka applications.. [1](#)

**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](#)

**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](#)
- Beta Release** A pre-release version of software intended for early access to new features that are still under development.. [2](#)
- 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](#)
- BYOC Bring Your Own Cloud** - A deployment model where a vendor's software is deployed and runs within a customer's cloud environment, allowing the customer to retain control over data residency and security policies.. [1](#)
- BYOD** Abbreviation for **Bring Your Own Device**, 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](#)
- 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](#)
- 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](#)
- 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 Contractual Obligations** - specific contractual obligations required to be in place by the [EU DORA](#) for regulated industries and their [ICT](#) suppliers.. *see* [DORA](#), [EU DORA](#) & [ICT](#)
- DR Disaster Recovery** 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 disasters such as fires, floods, cyberattacks (like ransomware), or massive regional power outages.. [1](#), *see* [HA](#) & [IT](#)
- DSAR Data Subject Access Request** - 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](#)
- EKS** Amazon's **Elastic Kubernetes Service** - A managed service that automates the deployment, scaling, and management of **Kubernetes** control planes and infrastructure on [AWS](#).. *see* [AWS](#)
- EU CRA EU 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.. *see* [CE Marking](#) & [EU](#)

**EU DORA** See [DORA](#). *see* [DORA](#)

**EU GDPR** Specifically the [EU](#) version of the [GDPR](#).. *see* [EU & GDPR](#)

**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.. *see* [IEC & ISO](#)

**HA** **High Availability** refers to a system design approach that ensures a service remains operational and accessible for a high percentage of time, even during component failures or routine maintenance. The goal of HA is to eliminate single points of failure so that if one part of the system breaks, another part immediately takes over without the user noticing a disruption.. [1](#)

**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](#)

**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** 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. *see* [IT](#)

**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](#)

**Milestone Release** A non-final release that may contain unfinished features or other issues.. [2](#)

**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](#)

**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](#)

- 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](#)
- PII Personally Identifiable Information** 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](#)
- 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](#)
- RoPA Record of Processing Activities - 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 Record of Processing Activities - 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](#)
- SCC Standard Contractual Clauses -** 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](#)
- 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](#)
- SLA A Service Level Agreement** is a legal or formal commitment between a service provider and a customer. It defines the minimum level of service expected and, crucially, the penalties (such as service credits or refunds) if those levels aren't met.. [1](#)
- SLO A Service Level Objective** 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](#)
- SOC System and Organization Controls -** A suite of audit reports produced by an independent third-party auditor (CPA firm) under the [AICPA](#) Trust Services Criteria, assessing the controls at a service organization relevant to security, availability, processing integrity, confidentiality, and privacy. SOC 2 Type II reports cover a defined period and provide evidence of the operating effectiveness of controls.. *see* [AICPA](#)
- Support Portal** Akka's online support ticketing/issue system.. [2](#)
- 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](#)
- 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 Trust Services Criteria** 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 United Kingdom -** 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](#)
- Your Application Services** In the context of Akka's policies, Your Application Services refers to application components or services developed by the customer to implement their business logic.. [1](#), [2](#)

# Index

Governance	
Governance - Availability Guarantee .....	1
Governance - Availability Guarantee Claims .....	2
Governance - Availability Guarantee	
Governance .....	1
Governance - Availability Guarantee Claims	
Governance .....	2