



Lightbend Inc, d.b.a Akka

# Cloud Terms of Service

2026-04-13

Version 1

# Contents

<b>Contents</b>	<b>i</b>
1.1 Introduction . . . . .	1
1.2 Referenced Frameworks and Standards . . . . .	1
1.3 Subscription . . . . .	1
1.3.1 Registration . . . . .	1
1.3.2 Grant of Use . . . . .	1
1.3.3 Termination or Expiration of Agreement and Effects of Termination . . . . .	2
1.3.4 User Restrictions . . . . .	2
1.3.5 Open Source Software . . . . .	3
1.4 Confidentiality . . . . .	3
1.4.1 Hold as Confidential . . . . .	3
1.5 Ownership . . . . .	3
1.5.1 Retained Ownership . . . . .	3
1.6 Customer Content . . . . .	4
1.6.1 Content . . . . .	4
1.7 Data Protection . . . . .	5
1.7.1 Privacy . . . . .	5
1.8 Disclaimer and Limitation of Liability . . . . .	5
1.8.1 Disclaimer . . . . .	5
1.8.2 Limitation of Liability . . . . .	5
1.9 Third Party Interactions . . . . .	6
1.9.1 Links . . . . .	6
1.9.2 Interactions . . . . .	6
1.9.3 Responsibility . . . . .	6
1.9.4 Refund or Credit . . . . .	7
1.10 Indemnifications . . . . .	7
1.10.1 Agreed Indemnifications . . . . .	7
1.11 Subscription Fees . . . . .	7
1.11.1 Payment of Fees . . . . .	7
1.12 Evaluation and Pre-Production Subscriptions . . . . .	8
1.12.1 Evaluation . . . . .	8
1.13 Support . . . . .	8
1.13.1 Akka Provides Support . . . . .	8
1.14 Term and Termination . . . . .	8
1.14.1 Effective Date . . . . .	8
1.14.2 Termination . . . . .	8
1.14.3 Survival . . . . .	9
1.14.4 Audit . . . . .	9
1.15 General . . . . .	9
1.15.1 Entire Agreement . . . . .	9
1.15.2 Severability . . . . .	9
1.15.3 Waiver . . . . .	9
1.15.4 Force Majeure . . . . .	9
1.15.5 No Third Party Beneficiaries . . . . .	9
1.15.6 Governing Law and Jurisdiction . . . . .	10
1.15.7 Marketing . . . . .	10
1.15.8 Notices . . . . .	10
1.15.9 Government Regulation . . . . .	10
1.15.10 Electronic Signatures . . . . .	11
1.16 Compliance . . . . .	11
Glossary . . . . .	12

## 1.1. Introduction

These Terms of Service (this “Agreement”) are between Lightbend, Inc. doing business as Akka (“Akka”), and the customer that desires to use the Cloud Services (as defined below) (“Customer”), and its employees and third parties (including affiliates, subsidiaries, employees, contractors and agents) (collectively, “End Users”), and is effective on the date this Agreement is accepted by Customer (“Effective Date”).

In order to use the Cloud Services, Customer must accept this Agreement. If Customer does not accept this Agreement, Customer is not permitted to use the Cloud Services under this Agreement. By agreeing to the terms and conditions set forth in this Agreement, Customer hereby represents and warrants to Akka Customer:

1. Is entering into this Agreement on its own behalf or on behalf of a third party (collectively with its affiliates, subsidiaries, agents, and End Users, the “Customer Company”);
2. Has the legal authority to bind the Customer Company to legal agreements;
3. Is at least eighteen (18) years old; and
4. Is not a Prohibited Person (as defined below).

[CCPA](#)

## 1.2. Referenced Frameworks and Standards

1. [Akka’s Internal Assurance Framework](#)

## 1.3. Subscription

### 1.3.1. Registration

To register to use the Cloud Services, Customer must provide Akka with the information requested in the registration process to create an account.

Akka will then grant Customer access to the applicable subscription(s) (“Subscriptions”). Customer must provide complete and accurate information during the registration process and will update Customer information to ensure it remains accurate.

Customer may not disclose usernames, passwords, or multi-factor authentication information to any unauthorized persons and must maintain such information in strict confidence. Customer shall ensure the Customer Company complies with all terms and conditions of this Agreement and applicable law, and Customer is responsible for all activities in Customer’s account, regardless of whether they are undertaken by Customer or the Customer Company, and Akka and its affiliates are not responsible for unauthorized access to Customer’s account.

Customer must contact Akka immediately if Customer thinks unauthorized activity occurred in Customer’s account or Customer’s account information is lost or stolen.

### 1.3.2. Grant of Use

Subject to the terms and conditions of this Agreement, Akka grants to Customer a limited, non-exclusive, non-assignable, non-sublicensable, non-transferable right to access and use the Cloud Services of ‘Akka’ (the “Cloud Services”) solely in the Territory (as defined herein), during the Term (as defined below), and in connection with Customer’s and/or the Customer Company’s lawful business operations.

Customer acknowledges and agrees its rights to access and use the Cloud Services are neither contingent upon the delivery of any future functionality or features, nor are they dependent upon any oral or written comments made by Akka with respect to future functionality or features.

For purposes hereof, “Territory” means the entire world, excluding countries that are the subject of embargoes or sanctions by the U.S., or with respect to which trade is otherwise prohibited by any instrumentality of the U.S.

### 1.3.3. Termination or Expiration of Agreement and Effects of Termination

Upon any expiration or termination of this Agreement, Customer's right to access and use the Cloud Services granted under this Agreement shall terminate immediately without any further action by Customer and/or Akka.

### 1.3.4. User Restrictions

Akka prohibits each Customer, whether acting itself, through the Customer Company or any other third party, from:

1. Selling, leasing, renting, loaning, licensing, distributing, sublicensing or otherwise transferring to a third party, in whole or in part, any software or documentation made available electronically as part of the Cloud Services (the "Documentation");
2. Decompiling, disassembling, translating, reverse engineering or otherwise attempting to derive or possess source code from the Cloud Services, in whole or in part, nor using any mechanical, electronic or other method to trace, decompile, disassemble, or identify the source code of the Cloud Services or encouraging others to do so, except to the limited extent, if any, that applicable law permits such acts notwithstanding any contractual prohibitions; provided, however, before a Customer exercises any rights to which it believes it is entitled under applicable mandatory law, the Customer must provide Akka with thirty (30) days' prior written notice thereof and provide all reasonably requested information to allow Akka to assess the Customer's claim and, at Akka's sole discretion, to provide alternatives that reduce any adverse impact on Akka's intellectual property or other rights;
3. Allowing access to, or permitting use of, the Cloud Services by any users other than the Customer and/or the Customer Company, and who, in each case, agreed in writing to abide by the terms of this Agreement, which writing the Customer agrees to provide to Akka upon receipt of its request. The Customer acknowledges it is liable for any failure by such employees and third party contractors to comply with the terms of this Agreement and/or any violation of usage restrictions (which shall be aggregated to the Customer across all such employees and third party contractors);
4. Creating, developing, licensing, installing, using, or deploying any third party software or services to circumvent or provide access, permissions or rights which violate the license keys embedded within the Cloud Services;
5. Modifying, enhancing, or otherwise changing the Cloud Services, or creating derivative works based upon the Cloud Services or Documentation;
6. Disclosing the results of any benchmark test of the Cloud Services to any third party without Akka's prior written approval (in its sole discretion);
7. Removing, obscuring, altering, or changing any notice of copyright, trademark, license, or other proprietary rights which appear in the Cloud Services or Documentation;
8. Using the Cloud Services as part of a software as a service where the Customer and/or the Customer Company receives payment for such software as a service or in any other resale capacity other than with respect to the use of the Customer's and/or the Customer Company's products; provided that, the Cloud Services shall not be used for purposes of competitive analysis, the development of a product or service that competes with the Cloud Services, or any other purpose that is, or reasonably could be, to Akka's commercial disadvantage;
9. Copying or otherwise reproducing the Cloud Services, the Documentation, or any materials provided in connection therewith except as expressly permitted herein;
10. Copying or embedding elements of the accessible code contained in the Cloud Services into other applications;
11. Performing or facilitating any act which, directly or indirectly, causes to be transmitted to, uploaded or downloaded by, Akka or any other end user any software viruses, worms, Trojan horses, time bombs, trap door or any other computer code, files or programs or repetitive requests for information designed to interrupt, destroy, or limit the functionality of any computer software or hardware or telecommunications equipment or to diminish the quality of, interfere with the performance of, or impair the functionality of the Cloud Services;
12. Using any robot, spider, scraper or other automated means to access the Cloud Services and collect content for any purpose without Akka's express written permission;
13. Using the Cloud Services for any illegal purpose or otherwise in violation of any applicable laws;
14. Using with, or distributing the Cloud Services to, any person located outside of the Territory or that is named on the U.S. Treasury Department's listing of specially designated nationals and blocked persons, or is otherwise blacklisted by any instrumentality of the U.S. (each such person, a "Prohibited Person"); or

15. Circumventing or attempting to circumvent any methods employed by Akka to control use of or access to the components, features or functions of the Cloud Services, or to prevent unauthorized use of the Cloud Services, including, but not limited to, breaching the firewall, cracking encryption codes, altering or disabling Akka's antivirus programs and protocols, or otherwise altering or disabling any other security mechanism used in the systems providing the Cloud Services.

### **1.3.5. Open Source Software**

The Cloud Services may include individual open source software components, each of which has its own copyright and its own applicable license conditions. These open source software components are licensed under the terms of the applicable open source license conditions and/or copyright notices.

## **1.4. Confidentiality**

### **1.4.1. Hold as Confidential**

Each party agrees to hold as confidential and not use or disclose for any purpose other than the performance of its obligations under this Agreement any information provided or disclosed by, or otherwise made viewable by the other party that reasonably should be understood to be confidential or proprietary to such other party in light of the nature of the information or the circumstances surrounding its disclosure.

Notwithstanding the foregoing:

1. The receiving party may disclose such information of the other party to the extent required to comply with binding orders of governmental entities that have jurisdiction over it; provided that, if legally permissible, such party provides the other party with reasonable written notice of such required disclosure in order to allow such other party the ability to seek a protective order or other appropriate remedy; and
2. To the extent the disclosing party provides such information on a non-confidential basis or in connection with Section 1.15.7 below, such information shall not be considered confidential and subject to the protections set forth in this section.

All of a party's information described herein shall be returned to such party upon its request; provided, however, the receiving party may retain one (1) archival copy thereof.

Notwithstanding the foregoing, nothing set forth herein shall be construed to prohibit Akka, its employees and agents from retaining, claiming ownership over, and/or using any:

1. General skills, know-how, expertise, generalized ideas, concepts, know-how, methods, techniques or skills gained or learned during the course of performing its obligations under this Agreement; and/or
2. Benchmarking, statistical, research and marketing analyses, surveys, reports and studies based on aggregated, blinded, non-personally identifiable formats of such information that do not identify, reference or imply an association with Customer or the Customer Company.

## **1.5. Ownership**

### **1.5.1. Retained Ownership**

As among Customer and Akka, Akka and its licensors shall retain ownership of the Cloud Services and all intellectual property and proprietary rights, title, and interest in and to the Cloud Services, training materials, Documentation, and related works, including, but not limited to, any derivative works of, or improvements, enhancements, and/or extensions made to the foregoing.

Customer acknowledges and agrees on behalf of itself and the Customer Company that nothing in this Agreement shall limit Akka's right to provide the Cloud Services and its services to third parties, including, but not limited to, any third parties that may have use cases, customizations, configurations, or other uses or applications similar to, or identical to, those of Customer or the Customer Company.

## 1.6. Customer Content

### 1.6.1. Content

Customer is solely responsible for all content uploaded to the Cloud Services under Customer's account ("Customer Content").

Customer is responsible for properly configuring and using the Cloud Services and taking steps to maintain appropriate security, protection, and backup of Customer Content including, but not limited to, updating usernames and passwords regularly as may be required by Akka, limiting account access to authorized persons, and implementing reasonable internal security measures.

Customer acknowledges Akka may collect information about Customer's computer hardware and software, including, but not limited to IP addresses, browser types, domain names, access times, and referring website addresses ("Customer Content"). Customer hereby grants Akka and its affiliates and vendors a fully-paid, non-exclusive, Territory-wide, royalty-free, non-transferable right and license to use, copy, cache, publish, display, process, and store such Customer Content and Customer Content in order to provide the Cloud Services and for other ordinary course of business purposes, including electronic communications.

Customer recognizes and agrees that caching of or references to the Customer Content may not be immediately removed upon termination. In addition to the foregoing, Customer hereby grants Akka a non-exclusive, perpetual, Territory-wide, fully-paid up, royalty-free license to use aggregated, blinded, non-personally identifiable formats of Customer

Content that do not identify, reference or imply an association with Customer for the creation of benchmarking, statistical, research and marketing analyses, surveys, reports and studies. Akka Customer warrants and represents that Customer has the right to grant Akka the rights set forth above and that it will not contribute any Customer Content that:

1. Infringes, violates or otherwise interferes with any copyright or trademark of another party;
2. Reveals any trade secret, unless Customer owns the trade secret or has the owner's permission to post it;
3. Infringes any intellectual property right of another or the privacy or publicity rights of another;
4. Is libelous, defamatory, abusive, threatening, harassing, hateful, offensive or otherwise violates any law or right of any third party;
5. Contains a virus, trojan horse, worm, time bomb or other computer programming routine or engine that is intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or information;
6. Includes any:
  - a) Personal Health Information (as defined under the Health Insurance Portability and Accountability Act), unless it enters into a separate agreement with a supplier relating to the processing of such data;
  - b) Government issued identification numbers, including Social Security numbers, driver's license numbers and other state-issued identification numbers;
  - c) Financial account information, including bank account numbers;
  - d) Payment card data, including credit card or debit card numbers; or
  - e) Sensitive personal data (as described under Article 9 of the General Data Protection Regulation 2016/679 (the "EU GDPR")) and any national laws adopted pursuant to the EU GDPR, about residents of Switzerland or any member country of the European Union, including racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life or the commission or alleged commission of any crime or offense; or
7. Remains posted after Customer has been notified that such Customer Content violates any of the terms of this Agreement or any law or regulation. Akka may deactivate Customer's account and all data upon the expiration or termination of Customer's applicable Subscriptions.

## 1.7. Data Protection

### 1.7.1. Privacy

The parties agree to comply with Akka's data protection policy set forth at <https://trust.akka.io/privacy> as modified from time to time, and with all applicable state, federal, and international data privacy and protection laws including, but not limited to, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, the European (Withdrawal) Act 2018, and the EU GDPR.

## 1.8. Disclaimer and Limitation of Liability

### 1.8.1. Disclaimer

THE CLOUD SERVICES AND DOCUMENTATION ARE PROVIDED AS-IS AND AKKA AND ITS SUPPLIERS MAKE NO WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE OR PURPOSE, INTEGRATION, NON-INFRINGEMENT, TITLE, PERFORMANCE, AND ACCURACY AND ANY IMPLIED WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE.

AKKA DOES NOT WARRANT THE OPERATION OR USE OF THE CLOUD SERVICES WILL MEET CUSTOMER'S AND/OR THE CUSTOMER COMPANY'S REQUIREMENTS, OR WILL BE UNINTERRUPTED, ERROR-FREE, OR ENTIRELY SECURE.

CUSTOMER AND THE CUSTOMER COMPANY SHALL BEAR ALL RISK ASSOCIATED WITH ANY USE OF THE INTERNET OR OTHER MEANS OF COMMUNICATION OR DATA TRANSMISSION BY OR ON BEHALF OF CUSTOMER OR THE CUSTOMER COMPANY UNDER THIS AGREEMENT, INCLUDING WITH RESPECT TO ANY VIRUS OR HARMFUL CODE RESULTING THEREFROM, AND AKKA DISCLAIMS ALL LIABILITY AND RESPONSIBILITY IN CONNECTION WITH SUCH USE. CUSTOMER AGREES AND ACKNOWLEDGES ON BEHALF OF ITSELF AND THE CUSTOMER COMPANY THAT LOSS OF DATA AND RECORDS IS A RISK IN CONNECTION WITH THIS AGREEMENT AND, THEREFORE, AGREES TO CONFIGURE AND BACKUP ITS COMPUTER SYSTEM ENVIRONMENT TO PREVENT THE ACTIVITIES CONTEMPLATED HEREUNDER FROM CAUSING BUSINESS INTERRUPTION, LOSS OF COMPANY DATA, OR OTHER LOSS OR DAMAGE.

WITHOUT LIMITING THE GENERALITY OF THE FOREGOING DISCLAIMER, THE CLOUD SERVICES AND DOCUMENTATION ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE:

1. IN THE PLANNING, CONSTRUCTION, MAINTENANCE, CONTROL, OR DIRECT OPERATION OF HAZARDOUS ENVIRONMENTS THAT REQUIRE FAIL-SAFE PERFORMANCE, SUCH AS NUCLEAR OR CHEMICAL FACILITIES, AIRCRAFT OR OTHER MODES OF HUMAN MASS TRANSPORTATION, LIFE SUPPORT SYSTEMS, IMPLANTABLE MEDICAL EQUIPMENT, MOTOR VEHICLES, WEAPONS SYSTEMS, OR OTHER USES IN WHICH THEIR FAILURE COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE; OR
2. WITH ANY INFORMATION, DATA OR TECHNOLOGY GOVERNED BY THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS.

### 1.8.2. Limitation of Liability

EXCEPT TO THE EXTENT ARISING IN CONNECTION WITH THE RESILIENCE GUARANTEE POSTED AT: <https://trust.akka.io/resilience-guarantee> (THE "RESILIENCE GUARANTEE"), IN NO EVENT WILL AKKA OR ITS SUPPLIERS BE LIABLE UNDER THIS AGREEMENT FOR ANY INDIRECT, RELIANCE, PUNITIVE, SPECIAL, EXEMPLARY, LOST PROFITS, REMOTE, COVER INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND AND HOWEVER CAUSED (INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOST BUSINESS, LOST GOODWILL, LOST SAVINGS AND LOST PROFITS) WHICH MAY ARISE UNDER THIS AGREEMENT, EVEN IF AKKA AND/OR ITS SUPPLIERS WERE PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

EXCEPT TO THE EXTENT EXPRESSLY PROVIDED UNDER THE RESILIENCE GUARANTEE, IN NO EVENT WILL AKKA'S CUMULATIVE LIABILITY FOR ANY CLAIM ARISING IN CONNECTION WITH THIS AGREEMENT EXCEED THE GREATER OF THE AMOUNT PAID TO AKKA BY CUSTOMER UNDER THIS AGREE-

MENT OR ONE HUNDRED DOLLARS (USD 100). IN NO EVENT WILL AKKA'S SUPPLIERS HAVE ANY LIABILITY FOR ANY CLAIM ARISING IN CONNECTION WITH THIS AGREEMENT.

THE PROVISIONS OF THIS SECTION ALLOCATE RISKS UNDER THIS AGREEMENT BETWEEN CUSTOMER, AKKA AND AKKA'S SUPPLIERS. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS IN ITS ESSENTIAL PURPOSE.

NO CLAIM MAY BE ASSERTED BY CUSTOMER OR THE CUSTOMER COMPANY AGAINST AKKA AND/OR ITS SUPPLIERS MORE THAN TWELVE (12) MONTHS AFTER THE DATE OF THE CAUSE OF ACTION UNDERLYING SUCH CLAIM. SOLELY IF AND TO THE EXTENT REQUIRED IN ORDER TO MAKE THE LIMITATION OF LIABILITY SET FORTH IN THIS SECTION ENFORCEABLE UNDER APPLICABLE LAW OUTSIDE OF THE U.S., NOTHING SET FORTH IN THIS AGREEMENT WILL EXCLUDE OR LIMIT LIABILITY TO A GREATER EXTENT THAN IS PERMITTED BY APPLICABLE LAW OR SHALL EXCLUDE OR LIMIT LIABILITY FOR FRAUD, FRAUDULENT MISREPRESENTATION OR FOR DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE.

## **1.9. Third Party Interactions**

### **1.9.1. Links**

The Cloud Services may contain links to third party websites and services, and/or display advertisements for third parties (collectively, "Third Party Links and Ads"). Such Third Party Links and Ads are not under Akka's control, and Akka is not responsible for any Third Party Links and Ads.

Akka provides access to these Third Party Links and Ads only as a convenience to Customer, and does not review, approve, monitor, endorse, warrant, or make any representations with respect to Third Party Links and Ads.

### **1.9.2. Interactions**

Any business relationship, exchange of data or other interaction between Customer and a third party, and/or any purchase, download or use by Customer of any of the Third Party Links and Ads (each, a Third Party Interaction), is solely between Customer and such third party, and Customer hereby releases and holds Akka harmless from, and will look to such third party with regard to, any claims relating to or arising out of a Third Party Interaction.

When Customer clicks on any of the Third Party Links and Ads, the applicable third party's terms and policies apply, including the third party's privacy and data gathering practices, including with respect to the use of, ownership of, and/or license to, the right to use any data, information, and/or reports provided by such third party in connection with such Third Party Interaction.

Akka is not a party to, has no involvement or interest in, makes no representation, warranty or guaranty with respect to, and has no obligation in connection with, any communication, transaction, interaction, dispute or any relation whatsoever between Customer and any third party through the Cloud Services; including, but not limited to, interactions related to payment and delivery of items and services, and any other terms, conditions, warranties or representations associated with such Third Party Interactions.

### **1.9.3. Responsibility**

Customer hereby acknowledges and agrees that Customer is responsible solely for ensuring Customer's Third Party Interactions:

1. Comply with all applicable foreign, federal and state laws and regulations; and
2. Do not violate any term, condition, rule, procedure, policy or other guideline published by a third party with which Customer interacts.

Also, Customer agrees Customer will be responsible solely for any fees owed to a third party as a result of a Third Party Interaction. While Akka may recommend such a third party and/or rely on data or information provided or generated by such third party in the course of providing the Cloud Services,

Customer hereby acknowledges Akka specifically does not warrant the accuracy, reliability or completeness of any such data and information; and agrees Akka will not be liable for any acts or omissions based on Customer's reliance thereon or any loss or liability arising therefrom.

#### **1.9.4. Refund or Credit**

If there are any defects with any items or services purchased as a result of the Cloud Services, any returns and/or demands for refund or credit must be made directly to the party from which Customer purchased such item or service.

### **1.10. Indemnifications**

#### **1.10.1. Agreed Indemnifications**

Customer hereby agrees, on behalf of itself and the Customer Company, to defend and hold harmless Akka and its affiliates, subsidiaries, officers, directors, stockholders, employees, consultants, representatives, agents, successors, and assigns (collectively including Akka, the "Indemnified Parties") in and against any and all claims, actions, and proceedings, and to indemnify any and all of the Indemnified Parties from and against all losses, liabilities, sums of money, damages, expenses, costs (including, but not limited to, reasonable attorneys' fees) ("Losses"), in connection with such claims, actions, or proceedings, and arising from:

1. Customer and/or the Customer Company's (including any of its employees, officers, directors, stockholders, employees, consultants, representatives, agents, successors and assigns) (each, an Indemnifying Party) breach of any term, condition, representation, or warranty set forth in this Agreement;
2. An Indemnifying Party's violation of applicable law;
3. An Indemnifying Party's violation, infringement, or misappropriation of the intellectual property rights or other rights of any third party; and/or
4. An Indemnifying Party's gross negligence or willful misconduct.

Subject to Section 1.8.2 above, Akka hereby agrees to indemnify Customer from and against all Losses awarded by Akka in connection with the Resilience Guarantee.

### **1.11. Subscription Fees**

#### **1.11.1. Payment of Fees**

The Subscriptions currently offered by Akka are described at <https://akka.io/pricing>.

Customer agrees to pay Akka the applicable fees for the applicable Subscription. The Cloud Services may include features or services which have separate rules specific to the feature or service of the applicable Subscription.

Customer will comply, and shall cause the Customer Company to comply, with all laws, rules, and regulations applicable to the use of the Cloud Services and any additional feature or service used. Customer understands and agrees that Akka may change, suspend or discontinue any part or all of the Cloud Services. Akka will notify Customer of any material change to or discontinuation of the Cloud Services by email or via Akka's website. All invoices shall be paid in U.S. dollars and are due upon receipt.

Payments are non-refundable and shall be made without right of set-off or chargeback. If Customer does not pay an invoice when due, Akka may:

1. Charge interest at one percent (1%) per month on the unpaid balance; and
2. Suspend the performance of its obligations, and revoke (temporarily or permanently) the access granted, under this Agreement until such payment is received by Akka.

For amounts outstanding for longer than sixty (60) days after the invoice date, Customer will be responsible for and agrees to pay reasonable costs and expenses of collection, including, but not limited to, court and attorneys' fees and expenses. All fees and charges payable by Customer are exclusive of applicable taxes and duties, including VAT and

applicable sales tax. Customer will provide Akka any information Akka reasonably requests to determine whether Akka is obligated to collect VAT from Customer, including Customer's VAT identification number.

If Customer is legally entitled to an exemption from any sales, use, or similar transaction tax, Customer is responsible for providing Akka with legally sufficient tax exemption certificates for each taxing jurisdiction. Akka will apply the tax exemption certificates to charges under Customer's account occurring after the date Akka receives the tax exemption certificates. If any deduction or withholding is required by law, Customer will notify Akka and will pay Akka any additional amounts necessary to ensure that the net amount Akka receives, after any deduction and withholding, equals the amount Akka would have received if no deduction or withholding had been required.

Additionally, Customer will provide Akka with documentation showing that the withheld and deducted amounts have been paid to the relevant taxing authority.

## **1.12. Evaluation and Pre-Production Subscriptions**

### **1.12.1. Evaluation**

Akka may provide access to the Cloud Services for a limited time solely for evaluation purposes. In addition, some Cloud Services may be in pre-production, testing, or beta phase for the purpose of evaluating performance, identifying defects and obtaining feedback and Akka has no obligation to release a final version of such offerings. Evaluation and pre-production Subscriptions are offered on an as-is basis with no Support (as defined below). However, Customer may submit inquiries to Akka during the Subscription term and Akka will use reasonable efforts to respond.

## **1.13. Support**

### **1.13.1. Akka Provides Support**

Akka will provide support (Support) as described at <https://trust.akka.io/customer-support>. Akka may modify the Support policy from time to time.

## **1.14. Term and Termination**

### **1.14.1. Effective Date**

This Agreement shall commence on the Effective Date and continue until terminated as set forth in this Agreement (Term). Akka may terminate this Agreement by providing Customer with thirty (30) days' prior written notice. Akka may also terminate Customer's account and this Agreement, or suspend Customer's access to the Cloud Services, immediately if: (i) Akka changes the way Akka provides or discontinues any Cloud Service; (ii) Customer is late in payment or otherwise in breach of this Agreement; (iii) Akka reasonably determines, in its sole discretion, that Customer's and/or the Customer Company's use of the Cloud Services poses a risk to the Cloud Services; (iv) Akka reasonably determines, in its sole discretion, that Customer's and/or the Customer Company's use of the Cloud Services may be unlawful; or (v) Customer and/or the Customer Company has ceased to operate in the ordinary course, made an assignment for the benefit of creditors or similar disposition of Customer's and/or the Customer Company's assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution or similar proceeding. If Akka suspends Customer's right to access or use any portion or all of the Cloud Services, Customer remains responsible for all fees and charges Customer has incurred during the suspension and Customer will not be entitled to any credit or refund. Akka will use commercially reasonable efforts to restore Customer's access to the Cloud Services promptly following resolution of the cause of Customer's suspension. Upon termination, the right to access the Cloud Services granted in this Agreement will expire. Expiration or termination of this Agreement for any reason shall not relieve the parties of any obligation accruing prior to expiration or termination.

### **1.14.2. Termination**

Upon termination of this Agreement:

1. All Customer's rights under this Agreement immediately terminate; and
2. Customer remains responsible for all fees and charges Customer has incurred up to and including the date of termination.

Customer accounts and data are deleted thirty (30) days after the expiration or termination of applicable Subscriptions. Akka has no obligation to continue to store Customer's and/or the Customer Company's data for more than thirty (30) days after termination or expiration of the applicable Subscription or this Agreement.

Customer shall contact Akka prior to the end of such thirty (30) day period to request any retained Customer and/or the Customer Company data from Akka.

### **1.14.3. Survival**

Sections 1.3.4, 1.4, 1.5.1, 1.8, 1.9, 1.10, 1.11, 1.14, and 1.15 shall survive the termination of this Agreement.

### **1.14.4. Audit**

During the Term and for a period of one (1) year following the end of the Term, Customer agrees and covenants on behalf of itself and the Customer Company Akka and its auditors may inspect Customer's and/or the Customer Company's records relating to its reproduction and use of the Cloud Services for the purpose of verifying Customer's and the Customer Company's compliance with this Agreement.

## **1.15. General**

### **1.15.1. Entire Agreement**

This Agreement constitutes the entire agreement between the parties concerning the subject matter hereof. This Agreement supersedes all prior or contemporaneous discussions, proposals, and agreements between the parties relating to the subject matter hereof. Customer hereby acknowledges and agrees, on behalf of itself and the Customer Company, Akka may revise any term or condition set forth in this Agreement at any time without requiring Customer's consent, which modifications shall become effective upon delivery to Customer of notice thereof. By continued use of the Cloud Services by Customer and/or the Customer Company (including any of its personnel), Customer agrees, on behalf of itself and the Customer Company, to be bound by the then-current version of this Agreement. In the event a non-English version of this Agreement is created and there is a conflict of terms between such non-English version and the English version of this Agreement, the English version will govern.

### **1.15.2. Severability**

If any provision of this Agreement is held to be invalid or unenforceable, the remaining portions shall remain in full force and effect and such provision shall be enforced to the maximum extent possible so as to effect the intent of the parties and shall be reformed to the extent necessary to make such provision valid and enforceable.

### **1.15.3. Waiver**

No waiver of rights by Akka may be implied from any actions or failures to enforce rights under this Agreement.

### **1.15.4. Force Majeure**

Akka is not liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond Akka's reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, epidemics, pandemics, acts or orders of government, acts of terrorism, or war.

### **1.15.5. No Third Party Beneficiaries**

Unless otherwise specifically stated, the terms of this Agreement are intended to be and are solely for the benefit of Akka and Customer and do not create any right in favor of any third party.

### 1.15.6. Governing Law and Jurisdiction

This Agreement shall be governed by and interpreted in accordance with the laws of the State of California, without reference to any states' principles of conflicts of law. The provisions of the Uniform Computerized Information Transaction Act and the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement. Any disputes related to this Agreement shall be brought exclusively in the state or federal courts located in San Francisco County, California, and Customer hereby irrevocably consents to the jurisdiction of such courts and hereby waives all objections thereto. To the extent Customer is located outside of the U.S., any additional or alternative terms and conditions to those contained in the Agreement, and required to comply with applicable law, will be mutually agreed upon by Akka and Customer and set forth in a country-specific exhibit to the Agreement.

### 1.15.7. Marketing

Customer grants Akka the right to use and display Customer's and the Customer Company's name and logo in Akka's promotional materials, including, but not limited to, any use case studies in which Customer participates.

### 1.15.8. Notices

All notices must be in English. Akka may provide any notice to Customer under this Agreement by posting a notice on the website for the applicable Cloud Service or sending a message to the email address associated with Customer's account. Customer will be deemed to have received any email sent to the email address then associated with Customer's account when Akka sends such email, whether or not Customer actually receives the email. To give Akka notice under this Agreement, Customer must:

1. Email Akka at <mailto:legal@akka.io> or
2. send Akka Customer's notice by certified mail, return receipt requested, to Akka, Inc., Attention: Legal Department, 580 California St., San Francisco, California 94104 USA.

### 1.15.9. Government Regulation

Customer acknowledges that the Cloud Services is subject to export restrictions by the U.S. government and import restrictions by certain foreign governments.

Customer may not export or re-export the Cloud Services except in compliance with the U.S. Export Administration Act and the related rules and regulations and similar non-U.S. government restrictions, if applicable.

Customer shall not and shall not allow any third-party to remove or export from the United States or allow the export or re-export of any part of the Cloud Services or any direct product thereof:

1. Into (or to a national or resident of) any embargoed or terrorist-supporting country;
2. To any Prohibited Person;
3. To any country to which such export or re-export is restricted or prohibited, or as to which the U.S. government or any agency thereof requires an export license or other governmental approval at the time of export or re-export without first obtaining such license or approval; or
4. Otherwise in violation of any export or import restrictions, laws or regulations of any United States or foreign agency or authority. Customer agrees to the foregoing and warrants that it is not located in, under the control of, or a national or resident of any such prohibited country or on any such prohibited party list.

The Cloud Services is further restricted from being used for:

1. Terrorist activity; or
2. The design or development of nuclear, chemical, or biological weapons or missile technology without the prior permission of the U.S. government.

Customer shall at all times comply, and shall cause the Customer Company to comply, with all applicable laws and regulations in its performance under this Agreement, including without limitation any applicable anti-corruption laws.

### 1.15.10. Electronic Signatures

As a convenience and courtesy to Customer, Akka provides access to the Cloud Services online, which may require Customer to enter into agreements or receive notices electronically.

Accordingly, Customer acknowledges and agrees that by clicking I Agree or I Accept, or other similarly marked affirmative statement, in connection with the Cloud Services:

1. Customer agrees to conduct electronically the particular transaction into which it is entering, including, without limitation, entering into this Agreement;
2. Customer has read, understands, and agrees to be bound by, and to bind the Customer Company by, the electronic copy of electronic contracts, notices and records to which it is agreeing, including, without limitation, this Agreement;
3. Customer is capable of printing or storing a copy of electronic records of agreements to which it is agreeing, including, without limitation, this Agreement;
4. Customer is capable of printing or storing a copy of electronic records of transactions into which Customer enters, including, without limitation, this Agreement and any amendments hereto; and
5. Customer agrees on behalf of itself and the Customer Company, to receive electronically information about the agreements to which it is agreeing, including, without limitation, this Agreement. If Customer wishes to withdraw this consent, Customer should contact Akka at <mailto:privacy@akka.io>, in which case Akka shall have the right to terminate Customers use of the Cloud Services.

### 1.16. 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 d'information** The French National Agency for the Security of Information Systems. [Agence nationale de la sécurité des systèmes d'information](#) 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 d'accreditation** The French national accreditation body responsible for accrediting [Conformity Assessment Bodies](#) 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. [Organismo di Certificazione della Sicurezza Informatica](#) acts as the [National Cybersecurity Certification Authority](#) for Italy under the [EUCC](#) scheme.. *see* [EUCC](#) & [National Cybersecurity Certification Authority](#)
- Protection Profile** An implementation-independent set of [CC](#) security requirements for a category of product, used as a reusable baseline. Vendors may claim [Protection Profile](#) compliance within their [Security Target](#).. *see* [CC](#) & [Security Target](#)
- 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. [Security Assurance Requirements](#) are composed into [Evaluation Assurance Levels](#).. *see* [CC](#) & [Evaluation Assurance Level](#)
- Security Functional Requirement** A requirement drawn from [CC](#) Part 2 that specifies the intended security behaviour of the [TOE](#). [Security Functional Requirements](#) are stated in the [Security Target](#) and verified during the evaluation.. *see* [CC](#), [Security Target](#) & [TOE](#)
- Security Problem Definition** The section of a [Security Target](#) or [Protection Profile](#) that formally describes the threats, organisational security policies, and assumptions that the [TOE](#) is designed to address.. *see* [Protection Profile](#), [Security Target](#) & [TOE](#)
- Security Target** A document defining the security problem, objectives, and summary of security specifications for a specific [TOE](#). The [Security Target](#) is the primary artefact evaluated and certified under [CC](#).. *see* [CC](#) & [TOE](#)
- TOE Summary Specification** A section of the [Security Target](#) that describes how the [TOE](#) satisfies each of its [Security Functional Requirements](#), bridging the security requirements and the implemented product.. *see* [Security Functional Requirement](#), [Security Target](#) & [TOE](#)
- United Kingdom Accreditation Service** The sole national accreditation body for the United Kingdom, responsible for accrediting [Conformity Assessment Bodies](#) and other conformity assessment organisations. Relevant to [EUCC](#) evaluations conducted by UK-based [Conformity Assessment Bodies](#) under mutual recognition arrangements.. *see* [Conformity Assessment Body](#) & [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** Artificial Intelligence - A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.. 1
- 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 Management System – 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 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** Assurance Life Cycle. [1](#)
- 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](#)
- API** **A**pplication **P**rogramming **I**nterface - A set of defined rules and protocols that enables secure communication and data exchange between distinct software systems or components.. [1](#)
- 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 **G**roup – 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** **Cloud Controls Matrix** – a cybersecurity control framework developed by the [CSA](#) that provides security controls mapped to leading industry standards for cloud environments.. *see* [CSA](#)
- CCPA** The **California Consumer Privacy Act**, a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.. [1](#)
- CD** **Continuous Deployment** - 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](#)
- CLI** **Command Line Interface** - A text-based interface allowing users to control an operating system or application by typing commands, commonly used for scripting, automation, and remote system management.. [1](#)
- CNAPP** **Cloud-Native Application Protection Platform** – 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** **Certified Public Accountant** - 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** **Cloud Security Alliance** – 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 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.. *see* [HA](#) & [IT](#)
- DRP** **Disaster Recovery Plan** – a documented set of procedures to recover and restore [IT](#) systems, data, and operations following a disruptive event.. *see* [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](#)
- DVS** Development Security. [1](#)
- 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** **A**mazons **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** **A**mazons **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** **E**U **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** **g**RPC - 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** Information and Communication Technology Security – 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** 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](#)
- LLM** Large Language Model – 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** Model Governance Framework – 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** Machine Learning – 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** Network Access Control List - 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** Network and Information Systems 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](#)
- 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. [1](#)
- NVD** National Vulnerability Database - 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** Office of the Privacy Commissioner – 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 **Personal Data Protection Act** – 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** **AWS Personal Health Dashboard** - 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** **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](#)
- PIMS** **Privacy Information Management System** — A management system for establishing, implementing, maintaining, and continually improving an organisation's 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** **Relational Database Service** - 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** **Representational State Transfer** - 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** **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](#)
- S3** **Simple Storage Service** - 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** **Security Assertion Markup Language** - 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** **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](#)
- 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](#)
- SCP** **Service Control Policy** - 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** **Security Domain** - 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](#)

- SLA** A **S**ervice **L**evel **A**greement 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 **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** **S**ecurity of **C**ritical **I**nfrastructure **A**ct 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** **A**WS **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** **T**he **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](#)
- VPC** A private, isolated network environment that can be established within various major cloud providers (e.g., AWS, GCP, Azure). Used as a general term to refer to such private network environments, not exclusively to Amazon Web Services' specific implementation.. [1](#)

# Index

Terms	
Terms - Confidentiality	3
Terms - Customer Content	4
Terms - Data Protection	5
Terms - Disclaimer and Limitation of Liability	5
Terms - Evaluation and Pre-Production Subscriptions	8
Terms - General	9, 10
Terms - Indemnifications	7
Terms - Ownership	3
Terms - Subscription	1-3
Terms - Subscription Fees	7
Terms - Support	8
Terms - Term and Termination	8, 9
Terms - Third Party Interactions	6, 7
Terms - Confidentiality	
Terms	3
Terms - Customer Content	
Terms	4
Terms - Data Protection	
Terms	5
Terms - Disclaimer and Limitation of Liability	
Terms	5
Terms - Evaluation and Pre-Production Subscriptions	
Terms	8
Terms - General	
Terms	9, 10
Terms - Indemnifications	
Terms	7
Terms - Ownership	
Terms	3
Terms - Subscription	
Terms	1-3
Terms - Subscription Fees	
Terms	7
Terms - Support	
Terms	8
Terms - Term and Termination	
Terms	8, 9
Terms - Third Party Interactions	
Terms	6, 7