Last revised: October 18, 2019

AUTH0, INC.
FREE, DEVELOPER, AND DEVELOPER PRO TERMS OF SERVICE

These Terms of Service (this "**Agreement**") contain the terms under which Auth0 agrees to grant Customer access to and use of Auth0's online identity management platform. By indicating Customer's acceptance of this Agreement, executing a Sales Order that references this Agreement, or using Auth0's services or software, Customer agrees to be bound by this Agreement. If you are entering into this Agreement on behalf of an entity, such as the company you work for, then you represent to Auth0 that you have the legal authority to bind the Customer to this Agreement. If you do not have that authority or if Customer does not agree with the terms of this Agreement, then you may not indicate acceptance of this Agreement, and neither you nor Customer may use or access any of Auth0's service offerings or other services. The "Effective Date" of this Agreement is the date on which you first indicate your assent to the terms of this Agreement.

Background

Auth0 provides user authentication and user authorization solutions, by providing its customers with access to Auth0's on-line identity management platform and tools. Customer wishes to acquire a subscription-based license to access and use the identity management platform and tools, all as specified in one or more "Sales Orders" under and subject to this Agreement. Therefore, for good and valuable consideration, the receipt and sufficiency of which they each acknowledge, Auth0 and Customer agree to be bound by this Agreement.

Terms and Conditions

1. Definitions and Construction

1.1. Definitions. For the purposes of this Agreement, the following initially capitalized words are ascribed the following meanings:

"**Acceptable Use Policy**" means the Auth0 policy described in Section 12.

"**Administrative User**" means any individual who is an employee or independent contractor of Customer, its Affiliates, or its or their Customer Service Providers, and who is authorized by Customer to use the administrative features and functions of the Auth0 Platform to administer access to and use of Customer Applications.

"**Affiliate**" means any person, partnership, joint venture, corporation or other form of venture or enterprise, domestic or foreign, including subsidiaries, which directly or indirectly Control, are Controlled by, or are under common Control with a party. "**Control**" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and operating policies of the entity in respect of which the determination is being made, through the ownership of more than fifty percent (50%) of its voting or equity securities, contract, voting trust or otherwise.

"**Auth0 Platform**" means the computer software applications, tools, application programming interfaces (APIs), connectors, programs, networks and equipment that Auth0 uses to make the Subscription Services available to its customers.

"**Channel Partner**" means an entity that Auth0 has authorized as a "reseller" of Auth0's Subscription Services.

"**Channel Partner Sale Agreement**" means the order, agreement or other document between Customer and a Channel Partner for Customer's purchase of Subscription Services. Terms that apply to Customer's use of the Subscription Services when purchased from a Channel Partner are specified in Section 13.

"**Confidential Information**" has the meaning ascribed to it in Section 6.1.

"**Customer**" means the entity identified as such in the applicable Sales Order.

"**Customer Application**" means an application or web-based service developed or used by Customer (including its APIs), and which utilizes the Auth0 Platform to identify or authenticate users. Customer Applications are provided by Customer, and not by Auth0; "Customer Application" does not include the Auth0 Platform.

"**Customer Data**" means any data that Customer or its Users input into the Auth0 Platform for Processing as part of the Subscription Services, including any Personal Data forming part of such data.

"**Customer Service Provider**" means a third party, to the extent the third party is providing services to Customer.

"**Documentation**" means the software user and administrator manuals published by Auth0 at https://www.auth0.com/docs, regarding use of the Auth0 Platform, including additional, updated or revised documentation, if any.

"**End User**" means any individual who has been authorized by Customer to use the end user features and functionality of the Auth0 Platform as part of its obtaining access to and use of Customer Applications.

"**Entitlements**" means the license metrics and other scope limitations applicable to Customer's license rights to access and use the Subscription Services, as specified in the applicable Sales Order and the Pricing Page.

"**Identity Provider**" or "**IdP**" means a compatible third party online service or website that authenticates users on the Internet by means of publicly available APIs, such as Google, LinkedIn or Facebook. Customer may configure the Auth0 Platform to enable IdPs so that Users can use their IdP authentication credentials to authenticate into Customer Applications via the Auth0 Platform.

"**Intellectual Property Rights**" means all trade secrets, patents and patent applications, trademarks (whether registered or unregistered and including any goodwill acquired in such trade marks), service marks, trade names, copyrights, moral rights, database rights, design rights, rights in know-how, rights in Confidential Information, rights in inventions (whether patentable or not) and all other intellectual property and proprietary rights (whether registered or unregistered, any application for the foregoing, and all rights to enforce the foregoing), and all other equivalent or similar rights which may subsist anywhere in the world.

"**Over-Quota Collection Guidelines**" means the guidelines published by Auth0 at https://auth0.com/legal/ss-oq-collection-guidelines .

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Pricing Page**" means the Auth0 pricing page published at https://auth0.com/pricing .

"**Process**" or "**Processing**" means any operation or set of operations which is performed on Customer Data or on sets of Customer Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Renewal Term**" has the meaning ascribed to it in Section 8.

"**Sales Order**" means (i) in the case of Customers who subscribe to the Developer or Developer Pro pricing plans, the online checkout form submitted by Customer and accepted by Auth0, and (ii) if Customer is subscribing to the Free pricing plan, the sign-up page on which Customer assents to this Agreement. Each Sales Order becomes effective when Auth0 enters the completed form into its system. Each Sales Order is made part of this Agreement as described in Section 1.2.

"**Subscription Services**" means the Auth0 Platform service offerings to which Customer subscribes, together with, if applicable to the pricing program to which Customer has subscribed, the "Enterprise" Support Program, each as specified in the Pricing Page, the applicable Sales Order, and the Documentation.

"**Subscription Start Date**" means the date on which Auth0 enters the Sales Order into its system.

"**Subscription Term**" has the meaning ascribed to it in Section 8.

"**Supplemental Materials**" means sample code, and sample programs made available or supported by Auth0 or by third parties for use with the Auth0 Platform. Supplemental Materials are not required for use of the Subscription Services, and may be accessed and used by Customer in its sole discretion.

"**Support Program**" means the "Standard" Auth0 support and maintenance services program, applicable to Developer and Developer Pro subscriptions. Terms governing the Support Program are specified in the 'Additional Terms of Service – Support Program' referenced in Section 12. Customers with a "Free" subscription may participate in community support, but are not eligible for the Support Program.

"**Tenant**" means a logical isolation unit, or dedicated share of a particular Auth0 Platform instance; the dedicated share may be configured to reflect the needs of the specific Customer business unit using the share.

"**User**" means any Administrative User or End User.

The following words will be interpreted as designated: (i) "or" connotes any combination of all or any of the items listed; (ii) where "including" is used to refer to an example or begins a list of items, such example or items will not be exclusive; (iii) "specified" requires that an express statement is contained in the relevant document; (iv) "will" is, unless the context requires otherwise, an expression of command, not merely an expression of future intent or expectation; and (v) "may" is, unless the context requires otherwise, an expression of permission, but not an obligation.

1.2. Construction. This Agreement applies to the provision of all Subscription Services. The parties will enter into one or more Sales Orders that contain additional terms and conditions applicable to the provision of certain Subscription Services. Upon execution by the parties, each Sales Order will be incorporated into this Agreement.

2. Provision and Use of Subscription Services; Operational Issues

2.1. Provision of Subscription Services. During the Subscription Term, Customer may access and use the Auth0 Platform in accordance with this Agreement. Auth0 will make the Auth0 Platform available to Customer, and, if and as applicable to Customer's subscription, provide the Support Program. Auth0 makes Supplemental Materials available on or via the auth0.com website or from within the Auth0 Platform.

2.2. Customer's Account. Customer will designate one or more of its employees to be the point of contact with Auth0 for the management and support of the Subscription Services, and who will be responsible for establishing and managing Customer's use of the Subscription Services ("**Account**"), including the creation of authentication credentials to access Customer's Account. Customer is solely responsible for maintaining the status of its User base. Customer will safeguard all Administrative User authentication credentials in its possession or under its control. Customer is responsible for all activities that occur under the Account.

2.3. Customer's General Responsibilities. Customer and its Users are solely responsible for obtaining and maintaining their Internet access to the Subscription Services. Customer is solely responsible for the accuracy, quality and integrity of the Customer Data that Customer or its Users input into the Auth0 Platform. Customer must comply, and will ensure that its Administrative Users comply, with the Acceptable Use Policy referenced in Section 12 below. Customer is responsible for acts and omissions of its Administrative Users relating to this Agreement as though they were Customer's own.

2.4. Customer Application. Customer is solely responsible for the development, implementation, operation, support, maintenance and security of each Customer Application.

2.5. Identity Provider Services. The Auth0 Platform includes functionality that enables Customer, at Customer's option, to connect with certain IdP services or sites, via public facing APIs provided and controlled by the IdP. Any authentication information transmitted to or accessed by the Auth0 Platform from an IdP is considered Customer's Confidential Information under this Agreement and, to the extent within Auth0's possession or under Auth0's control, is subject to the data protection provisions of Section 7. If an IdP modifies its APIs or equivalents so that they no longer interoperate with the Auth0 Platform, or imposes requirements on interoperability that are unreasonable for Auth0, and if after applying reasonable efforts Auth0 is unable to overcome such modifications or requirements then, upon reasonable notice to Customer, Auth0 may cease or suspend its provision of interoperability between the Auth0 Platform and the affected IdP services or sites, without liability to Customer. Except for Auth0's obligations to protect authentication credentials obtained by the Auth0 Platform from an IdP, Auth0 has no responsibility for the acquisition, development, implementation, operation, support, maintenance or security of any IdP.

2.6. Customer Load Testing or Penetration Testing. Customer may conduct load testing or penetration testing on Customer infrastructure that interoperates with the Auth0 Platform as Customer determines necessary or advisable. To the extent any such testing affects or may reasonably be expected to affect the Auth0 Platform, Customer must comply with applicable testing policies located at https://auth0.com/docs/policies . Customer may not conduct any penetration testing or load testing on the Auth0 Platform without Auth0's prior written consent in each instance, and then only subject to such conditions as Auth0 reasonably requires. Auth0 may terminate any testing of the Auth0 Platform at any time, as Auth0 determines necessary or advisable to protect the Auth0 Platform's operation or integrity.

2.7. Backup and Restore. Auth0 will perform backups of Customer Data stored on the Auth0 Platform every six hours. Auth0 will assist Customer in recovering and restoring Customer Data to the Auth0 Platform as specified in

Auth0's then-current restoration policies (published at auth0.com/docs/policies). If Customer requires restoration services other than as a result of an Auth0 Platform non-conformance, then Auth0 may charge for recovery and restoration services at Auth0's then-current applicable rates, or such other rates as may be agreed in writing with Customer.

2.8. Technology Improvement. Auth0 may modify the Subscription Services and Auth0 Supplemental Materials as it determines necessary to reflect to changes in technology and information security practices. Auth0 will notify Customer in advance of any material changes. Auth0 may require Customer to utilize Auth0 or third party software updates in order to continue using some or all of the Subscription Services (but at no additional charge with respect to updates provided by Auth0). If Auth0 proposes to introduce any "Breaking Change" into the Auth0 Platform, then Auth0 will provide Customer at least six months' notice prior to Auth0's implementation of the Breaking Change, except in cases of emergency, such as critical vulnerability remediation, in which case Auth0 will provide as much prior notice as is reasonable in the circumstances. A "Breaking Change" means a change to the Auth0 Platform that, to Auth0's knowledge, will cause failures in the interoperation of the Auth0 Platform and Customer Applications. If a modification made by Auth0 materially reduces the features or functionality of the Subscription Services then, unless Auth0 has provided a substantially equivalent replacement, or made the modification (i) to address a security vulnerability, (ii) to remain compliant with applicable law, or (iii) to comply with changes in its third party certification standards (such as ISO 27001 and ISO 27018), and if Customer has prepaid for a 12 month subscription, Customer may, at any time within the 30 day period following Auth0's implementation of the modification, terminate any affected Sales Order by delivery of written notice to Auth0 to that effect and, within 30 days of such termination, Auth0 will refund to Customer a pro-rata amount of any affected Subscription Services fees prepaid to Auth0 and applicable to the unutilized portion of the Subscription Term for terminated Subscription Services. If Customer has prepaid for a monthly subscription, then Customer may elect not to renew its subscription.

3. License Grants and Proprietary Rights

3.1. License by Auth0. Subject to the terms and conditions of this Agreement, Auth0 hereby grants to Customer a non-exclusive, non-transferable, royalty-free, worldwide license, without right to sub-license, for the Subscription Term, to (a) access and use, and to permit its Users to access and use, the Auth0 Platform, in accordance with the Documentation, subject to the Entitlements, and (b) reproduce, modify, and distribute and display the Documentation, in each case solely for Customer's operations in its ordinary course of business. Auth0 reserves all other rights not expressly granted in this Agreement.

3.2. License by Customer. Customer hereby grants to Auth0 a non-exclusive, royalty-free license, without right to sub-license (except to its sub-processors, as required for the provision of the Subscription Services), to use the Customer Data, solely as necessary to perform the Subscription Services and as otherwise may be agreed in writing by Customer. Customer reserves all other rights not expressly granted in this Agreement.

3.3. Ownership of Intellectual Property Rights.

3.3.1. *Ownership and Use of Customer Data*. Customer retains all of its rights, title and interest and Intellectual Property Rights in and to the Customer Data and Customer Confidential Information. No ownership interest in the Customer Data or Customer Confidential Information is transferred or conveyed to Auth0 by virtue of this Agreement. Auth0 will use Customer Data and Customer Confidential Information only for purposes of providing the Subscription Services, unless otherwise authorized in writing by Customer.

3.3.2. *Auth0's Intellectual Property and Ownership Rights*. As between Customer and Auth0, Auth0 and Auth0's licensors retain and own all right, title and interest and all Intellectual Property Rights in and to the Subscription Services, Auth0's Confidential Information, and Auth0's Supplemental Materials, and all enhancements or improvements to, or derivative works of any of the foregoing created or developed by or on behalf of Auth0 (collectively, "Auth0 Intellectual Property"). Nothing in this Agreement transfers or conveys to Customer any ownership interest in or to the Auth0 Intellectual Property.

3.4. Suggestions. If Customer provides Auth0 with any suggested improvements or enhancements to the Subscription Services ("Suggestions"), then Customer also grants Auth0 a non-exclusive, perpetual, irrevocable, paid-up, royalty-free, worldwide, transferable license, with right to sublicense, to make, have made, sell, offer for sale, use, import, reproduce, distribute, display, perform, and make derivative works of the Suggestions.

3.5. Restrictions. Customer will not: (i) except to the extent, if any, permitted by applicable law or required by Auth0's licensors, reverse assemble, reverse engineer, decompile or otherwise attempt to derive source code from any of the Auth0 Platform; (ii) reproduce, modify, or prepare derivative works of the Auth0 Platform; or (iii) share, rent or lease the Subscription Services, or use the Subscription Services to operate any timesharing, service bureau or similar business or to license the Auth0 Platform as a standalone offering.

4. Compensation

4.1. Subscription Services Fees and Plans. The rates for the Subscription Services are as published on the Pricing Page. Subject to the "over-quota" provisions of Section 4.2 below, Customer's subscription plan for the Subscription Services is specified in the applicable Sales Order and Pricing Plan. Customer may not reduce Customer's commitment under the subscription plan specified in the Sales Order during the Subscription Term. Customer is not entitled to any refund of fees paid or relief from fees due if the volume of Subscription Services Customer actually uses is less than the volume Customer ordered, and Customer may not carry over any of the unused volume to Customer's next Subscription Term.

4.2. Over-Quota Use

4.2.1. *Use in Excess of Entitlements*. Subject to Section 4.2.2, if Customer's use of the Auth0 Platform exceeds Customer's then current Entitlements ("**Excess Use**") then, without limiting any other remedies available to Auth0, Auth0 may charge Customer for the excess use, by applying the fees applicable to the excess use (as solely determined by Auth0) ("**Over-Quota Fees**") against Customer's credit card on file with Auth0.

4.2.2. *Over-Quota Collection Guidelines*. Auth0 will follow its then-current Over-Quota Collection Guidelines in addressing Excess Use and charging Customer for Over-Quota Fees, unless Auth0 determines in its sole and absolute discretion that Customer is acting in bad faith. As more specifically described in the Over-Quota Collection Guidelines, Auth0 will notify Customer of Customer's Excess Use before charging Over-Quota Fees, and Auth0 will not charge Over-Quota Fees until the Excess Use has continued for the period specified in the Over-Quota Guidelines. In applying the Over-Quota Collection Guidelines, Auth0 will base the excess Fees upon the next pricing tier that Auth0 determines applicable to Customer's Excess Use.

4.2.3. *Changes to Subscription Plan*. Whenever Auth0 charges Over-Quota Fees, Customer's subscription plan, Sales Order and Entitlements will be deemed automatically increased to reflect the pricing tier that Auth0 applies.

4.2.4. *Enterprise Transition*. If Customer's Excess Use causes Customer to no longer qualify for the Free, Developer or Developer Pro plans published on the Pricing Page then, unless Customer promptly cures such Excess Use, Customer will work expeditiously and in good faith with Auth0 to transition to Auth0's Enterprise plan, and in any event within 60 days of Auth0's request.

4.3. Payment of Subscription Services Fees. Customer will pay Auth0 the fees for the Subscription Services monthly or annually in advance, as specified in the applicable Sales Order, via credit card. Auth0 will not invoice for Subscription Services. All Fees are stated and payable in US dollars. Customer hereby authorizes Auth0 or its agents and Customer's financial institution to charge any credit card submitted by Customer for all fees due and payable under this Agreement, including any and all Over-Quota Fees.

4.4. Sales Taxes, Etc. Customer will be responsible for any applicable sales, value-added, use and similar taxes, together with all customs and import duties, and similar levies and impositions ("**Taxes**") payable with respect to its acquisition of Subscription Services, or otherwise arising out of or in connection with this Agreement, other than taxes based upon Auth0's personal property ownership or net income. All Fees exclude Taxes. If Customer has tax-exempt status, Customer will provide written evidence of such status with its purchase orders or upon request by Auth0.

5. Warranties

5.1. Warranties. Auth0 warrants to Customer that:

5.1.1. *Performance Warranty*. During the Subscription Term, the Auth0 Platform, in the form provided by Auth0, will conform in all material respects to its applicable specifications set forth in the Documentation.

5.1.2. *Viruses*. Auth0 will use commercially reasonable efforts, using applicable current industry practices, to ensure that the Auth0 Platform, in the form provided by Auth0 to Customer under this Agreement, contains no computer virus, Trojan horse, worm or other similar malicious code.

5.1.3. *Support Program.* Auth0 will provide the Support Program in a good, professional and workmanlike manner, consistent with applicable industry standards.

5.1.4. *Infringement*. Auth0's provision to Customer of the Subscription Services does not infringe any third party patent existing under the laws of the United States, Canada, any member state of the European Economic Area, the United Kingdom, Australia, New Zealand, Singapore, Brazil, South Korea, India or Japan, or infringe any third party copyright, trademark or service mark, or result from misappropriation by Auth0 of any third party's trade secrets (collectively, an "**Auth0 Infringement**").

5.1.5. *Compliance with Law*. The Subscription Services, in the form provided or made available by Auth0, will comply with all laws applicable to Auth0.

5.2. Performance Remedy. If the Auth0 Platform fails to conform to the warranty set forth in Section 5.1.1 and Customer provides written notice of the non-conformance to Auth0 within the applicable Subscription Term then, as Customer's exclusive remedy and Auth0's sole obligation: Auth0 will either repair or, at its option, replace the non-conforming Auth0 Platform or, if Auth0 is unable to correct the non-conformance within 30 days of receipt of such written notice from Customer, Customer may terminate the applicable Subscription Services, and Auth0 will refund to Customer a pro-rata amount of any Subscription Services fees prepaid to Auth0 and applicable to the unutilized portion of the Subscription Term for the terminated Subscription Services.

5.3. Infringement Remedy. Customer's sole and exclusive remedy for any non-conformance with the warranty in Section 5.1.4 above will be Customer's defense and indemnification rights under Section 9.1 below, and Customer's termination rights under Section 8.2 below.

5.4. Bugs and Abatement; Scope. Without limiting the express warranties in this Section 5 or any express warranties specified in the Additional Terms of Service, Auth0 does not warrant that the Auth0 Platform or Subscription Services are completely free from all bugs, errors, or omissions, or will ensure complete security. THE WARRANTIES IN SECTIONS 5.1.1 AND 5.1.3 DO NOT APPLY TO ANY FREE SUBSCRIPTION, OR TO ANY AUTH0 SUPPLEMENTAL MATERIALS. Supplemental Materials developed, created or provided by third parties are made available AS IS, without warranty of any kind. The warranties in this Agreement are for the sole benefit of Customer, and may not be extended to any other person or entity.

5.5. Disclaimer Of Implied Warranties. Neither party makes any representation or warranty in connection with the Subscription Services, except as expressly warranted in this Agreement or the Additional Terms of Service. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS SPECIFICALLY WARRANTED IN THIS SECTION 5 OR THE ADDITIONAL TERMS OF SERVICE, EACH PARTY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY OF NON-INFRINGEMENT OR IMPLIED OBLIGATION TO INDEMNIFY FOR INFRINGEMENT, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, AND ANY STATUTORY REMEDY.

6. Confidential Information

6.1. Restrictions on use and Disclosure. Neither Auth0 nor Customer will disclose to any third party any information provided by the other party pursuant to or in connection with this Agreement that the disclosing party identifies as being proprietary or confidential or that, by the nature of the circumstances surrounding the disclosure, ought in good faith to be treated as proprietary or confidential (such information, "**Confidential Information**"), and will make no use of such Confidential Information, except under and in accordance with this Agreement. Each party may disclose Confidential Information to its Affiliates and service providers, and its Affiliates and service providers may use such information, in each case solely for purposes of this Agreement. Each party will be liable for any breach of its obligations under this Section 6 that is caused by an act, error or omission of any such Affiliate or service provider. Confidential Information includes information disclosed by the disclosing party with permission from a third party, and combinations of or with publicly known information where the nature of the combination is not publicly known. Auth0's Confidential Information includes information regarding Auth0 Platform, Auth0's processes, methods, techniques and know-how relating to identity management, user

authentication or user authorization, Documentation, road-maps, pricing, marketing and business plans, financial information, information security information, Auth0's ISMS Standards (defined in Section 7.4 below) statements and similar independent third party certifications, and Personal Data of Auth0 personnel. Customer's Confidential Information includes its proprietary workflows and processes, systems architecture, marketing and business plans, financial information, information security information, information pertaining to Customer's other suppliers, and Personal Data of Customer personnel. This Section 6 does not apply to Auth0's obligations regarding use and protection of Customer Data; those obligations are specified in Section 7 (Data Protection).

6.2. Exclusions. Except with respect to Personal Data, Confidential Information does not include information that the receiving party can establish: (i) has entered the public domain without the receiving party's breach of any obligation owed to the disclosing party; (ii) has been rightfully received by the receiving party from a third party without confidentiality restrictions; (iii) is known to the receiving party without any restriction as to use or disclosure prior to first receipt by the receiving party from the disclosing party; or (iv) has been independently developed by the receiving party without use of or reference to the disclosing party's Confidential Information.

6.3. Disclosure Required By Law. If any applicable law, regulation or judicial or administrative order requires the receiving party to disclose any of the disclosing party's Confidential Information (a "Disclosure Order") then, unless otherwise required by the Disclosure Order, the receiving party will promptly notify the disclosing party in writing prior to making any such disclosure, in order to facilitate the disclosing party's efforts to protect its Confidential Information. Following such notification, the receiving party will cooperate with the disclosing party, at the disclosing party's reasonable expense, in seeking and obtaining protection for the disclosing party's Confidential Information.

6.4. Independent Development. The terms of confidentiality under this Agreement will not limit either party's right to independently develop or acquire products, software or services without use of or reference to the other party's Confidential Information.

7. Data Protection

7.1. Regulatory Issues.

7.1.1. *Personal Data – Compliance with Applicable Law.* Customer may select the Personal Data it elects to input into and Process using the Auth0 Platform in its sole discretion; Auth0 has no control over the nature, scope, or origin of, or the means by which Customer acquires, Personal Data Processed by the Subscription Services. Subject to the Customer Consent Assurance (defined in Section 7.1.4 below), Auth0 will comply, and will ensure that its personnel comply, with the requirements of state, federal and national privacy laws and regulations governing Customer Personal Data in Auth0's possession or under its control and applicable to Auth0's provision of Subscription Services. Customer is solely responsible for ensuring that it complies with any legal, regulatory or similar restrictions applicable to the types of data Customer elects to Process with the Auth0 Platform.

7.1.2. *EU-US Privacy Shield Program*. Auth0 is certified under the EU-US Privacy Shield Program and will maintain such certification during the currency of the program or the Subscription Term, whichever is shorter. Auth0 will notify Customer if Auth0 no longer meets the certification requirements.

7.1.3. *ePHI*. If Customer is subject to US healthcare data protection laws (e.g., HIPAA), Customer may not use the Auth0 Platform to Process "electronic Protected Health Information".

7.1.4. *Data Consents*. Customer is solely responsible for obtaining, and represents and covenants that it has obtained or will obtain prior to Processing by Auth0, all necessary consents, licenses and approvals for the Processing of any Customer Data (and any other Personal Data provided by Customer) as part of the Subscription Services (the "**Customer Consent Assurance**").

7.1.5. *Regulator Inquiries and Court Orders.* If any regulator, or any subpoena, warrant or other court or administrative order, requires Auth0 to disclose or provide Customer Data to a regulator or to any third party, or to respond to inquiries concerning the Processing of Customer Data, Auth0 will promptly notify Customer, unless prohibited by applicable law.

7.2. Instructions. Auth0 will Process Customer Data only as necessary to provide the Subscription Services, and in accordance with Customer's written instructions. This Agreement, and Customer's use of the Auth0 Platform's features and functionality, are Customer's complete set of instructions to Auth0 in relation to the Processing of Customer Data.

7.2.1. *CCPA Restrictions.* The restrictions in this Section 7.2.1 apply for purposes of Customer Data that is (a) Personal Data, and (b) subject to the California Consumer Privacy Act of 2018, as amended from time to time.

7.2.1.1. Auth0 will not retain, use, or disclose Personal Data for any purpose other than as required for the specific purpose of performing the Services and for the business purposes described in Section 14.8 (Service Performance Analytics);

7.2.1.2. Auth0 will not sell Personal Data to any third party. For these purposes, "Sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means any Personal Data to any third party for monetary or other valuable consideration.

7.2.1.3. For clarity, the restrictions in this Section 7.2.1 include retention, use or disclosure of Personal Data by Auth0 outside of the direct business relationship between Auth0 and Customer.

7.2.1.4. Auth0 certifies that it understands the restrictions in this Section 7.2.1 and will comply with them.

7.3. Information Security. Auth0 will implement and maintain commercially reasonable technical and organizational security measures designed to meet the following objectives: (i) ensure the security and confidentiality of Customer Data in the custody and under the control of Auth0; (ii) protect against any anticipated threats or hazards to the security or integrity of such Customer Data; (iii) protect against unauthorized access to or use of such Customer Data; and (iv) ensure that Auth0's return or disposal of such Customer Data is performed in a manner consistent with Auth0's obligations under items (i)-(iv) above. Customer is solely responsible for consequences of Customer's decision not to adopt updates or best practices that Auth0 makes available to Customer.

7.4. Audits and Security Assessments. Auth0 is and will remain in compliance with its SOC-2 statement and, with effect from July 2018, the ISO 27001 and ISO 27018 standards (collectively, "**ISMS Standards**"), throughout the Subscription Term. Auth0 will cause its independent ISMS Standards certification auditors to verify the adequacy of the controls that Auth0 applies to the Subscription Services at least annually. Auth0 will provide Customer with copies of its ISMS Standards certifications applicable to Auth0's provision of Subscription Services, upon request by Customer. Auth0 will in addition provide such information regarding its information security systems, policies and procedures as Customer may reasonably request relating to Customer's due diligence and oversight obligations under applicable laws and regulations.

7.5. Data Export, Retention and Destruction. Customer may export Customer Data from the Auth0 Platform at any time during the Subscription Term, using the Auth0 Platform's then existing features and functionality. Customer is solely responsible for its data retention obligations with respect to Customer Data. Customer may delete Customer Data on its Tenants at any time. Auth0 will delete Customer's Tenants (and any data remaining on such Tenants) within 30 days of termination or expiration of the Subscription Term, and other Customer Data retained by Auth0 (if any). Auth0 is not obligated to delete copies of Customer Data retained in automated backup copies generated by Auth0, which Auth0 will retain for up to 14 months from their creation. Such backup copies will remain subject to this Agreement until the copy, or the Customer Data in the copy, is deleted.

7.6. Sub-Processors. Customer consents to Auth0's use of sub-processors to provide aspects of the Subscription Services, and to Auth0's disclosure and provision of Customer Data to those sub-processors. Auth0 publishes a list of its then-current sub-processors at https://auth0.com/legal ("Sub-Processor List"). Auth0 will require its sub-processors to comply with terms that are substantially no less protective of Customer Data than those imposed on Auth0 in this Agreement (to the extent applicable to the services provided by the sub-processor). Auth0 will be liable for any breach of its obligations under this Agreement that is caused by an act, error or omission of a sub-processor. Auth0 may authorize new sub-processors by provision of not less than 30 days' prior written notice to Customer, and by updating the Sub-Processor List. If Customer objects to the authorization of any future sub-processor on reasonable data protection grounds within 30 days of notification of the proposed authorization, and if Auth0 is unable to provide an alternative or workaround to avoid Processing of Customer Data by the objected to sub-processor within a reasonable period of time, not to exceed 30 days from receipt of the objection, then, at any time within expiration of such 30 days period, Customer may elect to terminate the affected Sales Order(s) without penalty, by notice to Auth0 to that effect.

7.7. Access by Auth0 Personnel. Auth0 will ensure that its personnel access Customer Data only when authorized by Auth0, and in accordance with Auth0's applicable controls. Access is typically required only in connection with Auth0's provision of the Support Program, and then only when necessary to resolve an issue. Auth0 will ensure that its personnel are subject to obligations of confidentiality with respect to Customer Data. Auth0 will not permit its personnel to access Customer Data unless they have passed a criminal and employment background check.

7.8. User Requests. If any User requests Auth0 to provide them with information relating to Processing of their Personal Data, or to make changes to their Personal Data, then Auth0 will promptly notify Customer of the request, unless otherwise required by applicable law. Customer may make changes to User data using the features and functionality of the Auth0 Platform. Auth0 will not make changes to User data except as agreed in writing with Customer.

7.9. Breach Notification. Auth0 will notify Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data in Auth0's possession or under its control (a "Security Breach") within 72 hours of Auth0's confirmation of the nature and extent of the same or when required by applicable law, whichever is earlier. Each party will reasonably cooperate with the other with respect to the investigation and resolution of any Security Breach including, in the case of Auth0, prompt provision of the following, to the extent then known to Auth0: (i) the possible cause and consequences of the Security Breach; (ii) the categories of Personal Data involved; (iii) a summary of the possible consequences for the relevant Users; (iv) a summary of the unauthorized recipients of the Customer Data; and (v) the measures taken by Auth0 to mitigate any damage. Upon confirmation of any vulnerability or breach of Auth0's security affecting Customer Data in Auth0's custody and control, Auth0 will modify its processes and security program as necessary to mitigate the effects of the vulnerability or breach upon such Customer Data. Insofar as the Security Breach relates to Customer, and except to the extent required otherwise by applicable law, Customer will have approval rights on notifying its Users and any third party regulatory authority of the Security Breach. All security breach or security compromise notifications will be via the Auth0 Platform dashboard or account center, and via email to the persons designated by Customer to receive notices in the Auth0 Platform dashboard or account center.

7.10. Territorial Restrictions. Auth0 will Process Customer Data within the AWS regions selected by Customer upon creation of the applicable Tenant. In addition, some processing of Customer Data will occur on infrastructure located in the European Union (currently Germany, with failover to the Republic of Ireland). Dashboard data may be viewed (but not stored) in the United States. Auth0 personnel may access Customer Data from any location for purposes of providing Support Subscription Services (subject to the restrictions described in Section 7.7 above).

7.11. Data Processing Addendum for GDPR. If and to the extent Customer uses the Auth0 Platform to Process Personal Data that is subject to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (known as the General Data Protection Regulation) ("**GDPR**") then the additional data protection provisions specified in Exhibit A to this Agreement apply.

8. Term; Termination of Sales Orders

8.1. General. This Agreement will commence on the Effective Date and will continue in effect until terminated in accordance with Section 8.2 or 8.3 below.

8.2. Termination On Breach. In the event of a material breach of the Agreement by either party, the non-breaching party may terminate the Agreement or any Sales Order affected by the breach by giving the breaching party written notice of the breach and the non-breaching party's intention to terminate. If the breach has not been cured within the period ending 30 days after such notice, and if the non-breaching party provides written notice of termination to the breaching party ("Termination Notice"), then this Agreement or any such Sales Order will terminate within the time period specified in the Termination Notice. Notwithstanding the foregoing, (a) Customer's failure to pay any overdue fees and expenses within 10 days of Auth0 notifying Customer of the overdue payment, (b) Customer's failure to provide a valid credit card within 10 days of Auth0's request, or (c) Customer's use of two or more Tenants in a manner that Auth0 in its sole discretion determines is to avoid or reduce fees payable to Auth0, and which is not cured within 10 days of notification by Auth0, will each constitute a material breach of this Agreement; the default 30 day cure period described above is inapplicable to any breach under items (a), (b) or (c)

above. If Customer has not cured a material breach within the applicable cure period (if any) then, without limiting Auth0's rights to terminate as described above, Auth0 may, on not less than 5 business days' prior written notice to Customer, in its sole discretion, and without prejudice to its other rights following material breach and failure to cure, until such breach has been cured in full, do all or any of the following: (i) downgrade Customer to a "Free" Plan (as described in the Pricing Page; or (ii) suspend performance of some or all of Auth0's obligations to provide Subscription Services under this Agreement. If Customer terminates this Agreement or any Sales Order for breach in accordance with this Section 8.2, then Auth0 will refund to Customer a pro-rata amount of any affected Subscription Services fees prepaid to Auth0 and applicable to the unutilized portion of the Subscription Term for terminated Subscription Services.

8.3. Termination for Convenience. The parties acknowledge and agree that each Subscription Term is priced as a minimum term, and may not be terminated for convenience.

8.4. Subscription Term and Renewal. Each subscription term for Subscription Services will commence on the Subscription Start Date, and will continue for the period for which Customer has prepaid Auth0 using the online checkout (for example, for one month or for one year) (an "**Initial Term**"). Upon expiration of the Initial Term the Initial Term will automatically renew for successive periods of the same length as the Initial Term (each, a "**Renewal Term**"), at the then-current rates specified in the Pricing Page, or such other rates as may be mutually agreed in writing between Auth0 and Customer. Customer's credit card will be automatically debited for the fees payable for each Renewal Term at the beginning of each Renewal Term. The Initial Term and each Renewal Term are individually referred to in these Terms as the "**Subscription Term**". Customer may terminate the Subscription Term at any time by deleting its Account via the Auth0 Platform dashboard; the termination will become effective at the end of the then-current period for which Customer has prepaid, and the Subscription Term will not renew. ***Customer acknowledges that its subscription will automatically renew, and Customer's credit card will continue to be charged, until Customer terminates its subscription as specified in this Section 8.4.1.*** Auth0 may terminate the Subscription Term upon expiration of the Initial Term or the then-current Renewal Term, by provision of not less than 10 days' prior notice to Customer.

8.5. Fulfillment of Obligations on Termination. Except as otherwise specified in this Agreement or any Additional Terms of Service, termination of the Agreement or of any Subscription Services will not entitle Customer to any refund of or relief from payment of any Subscription Services fees paid or payable under this Agreement.

8.6. Post Termination Obligations. Following any termination of the Agreement or any Sales Order, each party will, within 30 days of such termination, (i) immediately cease use of any Confidential Information of the other communicated for the purposes of this Agreement or such Sales Order, and (ii) return or destroy (and certify destruction of) all copies of any Confidential Information of the other party disclosed under the Agreement or such Sales Order within 30 days of such termination, subject to each party's customary backup and archival processes.

8.7. Suspension.

8.7.1. *Critical Threats*. If Auth0 determines that Customer's or any of its Users' use of the Subscription Services or of any Identity Provider service or site poses an imminent threat to (i) the security or integrity of any Customer Data or the data of any other Auth0 customer, or (ii) the availability of the Auth0 Platform to Customer or any other Auth0 customer (collectively, a "Critical Threat"), then Auth0 will immediately attempt to contact Customer to resolve the Critical Threat. If Auth0 is unable to immediately contact Customer, or if Auth0 contacts Customer but Customer is unable to immediately remediate the Critical Threat, then Auth0, acting reasonably in the circumstances then known to Auth0, may suspend Customer's and its Users' use of the Auth0 Platform until the Critical Threat is resolved and Auth0 is able to restore the Subscription Services for Customer.

8.7.2. *Other Non-Compliance*. If Auth0 determines that Customer's or any of its Users' use of the Subscription Services or of any Identity Provider service or site do not comply with applicable law or with the Acceptable Use Policy, or if they subject Auth0 or any of its sub-processors to liability to any third party, or if they infringe or are alleged to infringe any third party Intellectual Property Rights (collectively, a "Non-Compliance"), and if Customer has not remediated the Non-Compliance within 5 days of notification by Auth0, then Auth0 may suspend Customer's and its Users' use of the Auth0 Platform until the Non-Compliance is resolved and Auth0 is able to restore the Subscription Services for Customer. If Auth0 determines that the Non-Compliance is incapable of cure, then Auth0 may immediately terminate its provision of Subscription Services to Customer.

8.8. Survival. The provisions of Sections 1, 3.3-3.5, 6, 7, 8.5-8.8, 9-11 and 14 of this Agreement will survive any termination or expiration of this Agreement.

9. Indemnification

9.1. Auth0's Infringement Indemnification.

9.1.1. *Defense and Indemnity*. If any third party makes any claim against Customer that, if true, would constitute an Auth0 Infringement (defined in Section 5.1.4) then, upon notification of such claim, Auth0 will, at its sole cost and expense, defend Customer against such claim and any related proceeding brought by such third party against Customer, and indemnify Customer from and against all damages, fines and penalties finally awarded against Customer or agreed to be paid by Customer in a written settlement approved in writing by Auth0, and resulting from the Auth0 Infringement. Auth0's obligations under this Section 9.1.1 are subject to Customer's compliance with the "Indemnification Conditions" (defined below).

"**Indemnification Conditions**" means the following conditions with which a party must comply in order to be entitled to defense or indemnification under the Agreement by the other party: (i) the indemnified party notifies the indemnifying party in writing of any claim that might be the subject of indemnification promptly after any executive officer of the indemnified party or member of the indemnified party's legal department first knows of the claim, provided, however, that no failure to so notify an indemnifying party will relieve the indemnifying party of its obligations under this Agreement except to the extent that such failure materially prejudices defense of the claim, and except to the extent of damages incurred by the indemnifying party as a result of the delay; (ii) the indemnifying party is given primary control over the defense and settlement of the claim (subject to the foregoing, the indemnified party may nonetheless participate in the defense at its sole cost and expense); (iii) the indemnified party makes no admission of liability (except as required by applicable law) nor enters into any settlement without the indemnifying party's prior written agreement (not to be unreasonably withheld); (iv) the indemnified party provides such assistance in defense of the proceeding as the indemnifying party may reasonably request, at the indemnifying party's reasonable expense; and (v) the indemnified party uses all commercially reasonable efforts to mitigate its losses.

9.1.2. *Auth0's Mitigation Rights*. If any Subscription Services become (or in Auth0's opinion are likely to become) the subject of any infringement or misappropriation claim, Auth0 may, and if Customer's use of the Subscription Services is enjoined, Auth0 must, at its sole expense, either: (i) procure for Customer the right to continue using the relevant Subscription Services; (ii) replace or modify the relevant Subscription Services in a functionally equivalent manner so that they no longer infringe; or (iii) terminate the applicable Sales Order or Customer's rights to use affected Subscription Services, and refund to Customer a pro-rata amount of any subscription fees prepaid to Auth0 and applicable to the unutilized portion of the Subscription Term for the terminated Subscription Services.

9.1.3. *Exclusions*. Notwithstanding the foregoing, Auth0 will have no obligation with respect to any infringement or misappropriation claim to the extent based upon (i) any use of the Subscription Services not in accordance with their applicable license rights, (ii) the combination of the Subscription Services with other products, equipment, software, services or data not supplied by Auth0 where the infringement would not have occurred but for such combination, or (iii) any Customer Data.

9.2. Customer's Consent Indemnification.

9.2.1. *Defense and Indemnity*. If any third party makes any claim against Auth0 that, if true, would constitute a non-conformance with the Customer Consent Assurance (defined in Section 7.1.4) then, upon notification of such claim, Customer will, at its sole cost and expense, defend Auth0 against such claim and any related proceeding or investigation brought by such third party against Customer, and Customer will indemnify Auth0 from and against all damages, fines and penalties finally awarded against Auth0 or agreed to be paid by Auth0 in a written settlement approved in writing by Customer, and resulting from the non-conformance. Customer's obligations under this Section 9.2.1 are subject to Auth0's compliance with the Indemnification Conditions.

9.2.2. *Mitigation Rights*. If Customer Data is, or in Customer's reasonable opinion is likely to become, the subject of a claim of non-conformance with the Customer Consent Assurance, then Customer will have the right to: (i) procure the rights necessary for Customer and Auth0 to continue to Process the affected Customer Data; (ii)

modify the Customer Data so that there is no longer a non-conformance; or (iii) delete or otherwise remove the non-conforming Customer Data from the Auth0 Platform.

9.2.3. *Exclusions*. Notwithstanding the foregoing, Customer will have no obligation under this Section 9.2 or otherwise with respect to any claim of non-conformance with the Customer Consent Assurance to the extent based upon Auth0's Processing of the affected Customer Data other than in accordance with this Agreement.

9.3. Improper Use of Auth0 Platform. Customer will indemnify and hold Auth0 harmless from any claims, damages, losses, judgments, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or in connection with any non-compliance by Customer or its Administrative Users with the Acceptable Use Policy.

10. Limitations and Exclusions of Liability

10.1. Exclusion of Certain Claims. SUBJECT TO SECTION 10.3, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR EXEMPLARY DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE (INCLUDING ANY DAMAGES FOR LOSS OF DATA, GOODWILL, REVENUE OR PROFITS), EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, ARISING OUT OF (i) THE PERFORMANCE OR NON-PERFORMANCE OF THIS AGREEMENT OR ANY RELATED AGREEMENT, OR ANY SOFTWARE, PRODUCTS OR SERVICES PROVIDED HEREUNDER, OR (ii) ANY CLAIM, CAUSE OF ACTION, BREACH OF CONTRACT OR ANY EXPRESS OR IMPLIED WARRANTY, UNDER THIS AGREEMENT, ANY RELATED AGREEMENT OR OTHERWISE, MISREPRESENTATION, NEGLIGENCE, STRICT LIABILITY, OR OTHER TORT.

10.2. Limitation of Liability. Subject to Section 10.3, neither party's maximum aggregate liability arising out of this Agreement or any related agreement will in any event exceed the greater of US $25, or the fees paid to Auth0 under the Sales Order giving rise to the claim during (i) if Customer is pre-paying for Subscription Services on a monthly basis, the one month period, or (ii) if Customer is pre-paying for Subscription Services on an annual basis the twelve month period, immediately preceding the aggrieved party's first assertion of any claim against the other, regardless of whether any action or claim is based in contract, misrepresentation, warranty, indemnity, negligence, strict liability or other tort or otherwise.

10.3. Exceptions. Sections 10.1 and 10.2 do not apply to liability or loss which may not be limited by applicable law. Any amounts payable by an indemnified party to a third party pursuant to a judgment or to a settlement agreement approved in writing by an indemnifying party, liability for which falls within the indemnifying party's indemnification obligations under this Agreement, and all fees payable by Customer under this Agreement, will be deemed direct damages for purposes of this Section 10. Section 10.2 does not apply to (i) each party's defense and indemnification obligations, (ii) any infringement or misappropriation by Customer of any of Auth0's Intellectual Property Rights, (iii) Customer's obligations to pay fees and expenses when due and payable under this Agreement, or (iv) either party's obligations under Section 6 (Confidential Information).

10.4. General. Each party agrees that these exclusions and limitations apply even if the remedies are insufficient to cover all of the losses or damages of such party, or fail of their essential purpose and that without these limitations the fees for the Subscription Services would be significantly higher. Neither party may commence any action or proceeding under this Agreement more than two years after the occurrence of the applicable cause of action.

11. Dispute Resolution

11.1. Governing Law and Venue. This Agreement will be governed by and interpreted in accordance with the internal laws of the states or countries specified in the table below, without regard to conflicts of laws principles. In the event of any controversy or claim arising out of or relating to this Agreement, or its breach or interpretation, the parties will submit to arbitration as specified in the table below. Each party waives all defenses of lack of personal jurisdiction and inconvenient forum.

If the Customer's address in the Sales Order is in:	The governing law is that of:	The arbitration bodies having exclusive jurisdiction are:
The USA, Mexico, Canada or any country in Central or South America or the Caribbean	Washington, USA, and controlling United States federal law	Arbitration in Seattle, Washington, USA under the Commercial Arbitration Rules and the Optional Rules for Emergency Measures of Protection of the American Arbitration Association; those rules are incorporated by reference in this clause.[1]

Any country in Europe, the Middle East, or Africa	England	Arbitration in London, England under the Rules of the London Court of International Arbitration (LCIA); those rules are incorporated by reference in this clause.[1]
Any country located in Asia or the Pacific region, including Australia and New Zealand	England	Arbitration in Singapore in accordance with the Arbitration Rules of the Singapore International Arbitration Centre then in force; those rules are incorporated by reference in this clause.[1]

Note 1: The Tribunal will consist of one independent, disinterested arbitrator. The language of the arbitration will be English. The determination of the arbitrator will be final, conclusive and binding. Judgment upon the award rendered may be entered in any court of any state or country having jurisdiction.

12. Additional Terms of Service

The following additional terms and conditions ("**Additional Terms of Service**") apply to Customer's use of the Subscription Services, and are incorporated into this Agreement by this reference. The Additional Terms of Service are published at https://www.auth0.com/legal :

- Support Program (does not apply to customers subscribing to the Free program)
- Acceptable Use Policy
- Modification Policy

13. Purchase Through Channel Partners

13.1. Applicability. This section 13 only applies to Customers purchasing Subscription Services through a Channel Partner. If Customer is uncertain as to the applicability of this section to its purchase of Subscription Services, Customer should contact Auth0 for further information.

13.2. Channel Partners. If Customer acquired the Subscription Services from a Channel Partner, then this Agreement is not exclusive of any rights Customer obtains under the Channel Partner Sale Agreement; however, if there is any conflict between the provisions of this Agreement and the Channel Partner Sale Agreement, then the provisions of this Agreement prevail. If a Channel Partner has granted Customer any rights that Auth0 does not also directly grant to Customer in this Agreement, or that conflict with this Agreement, then Customer's sole recourse with respect to such rights is against the Channel Partner.

13.3. Term and Renewal. If Customer ordered the Subscription Services through a Channel Partner, then Section 8.4 is inapplicable, and the Subscription Term will begin on the Subscription Start Date and, subject to the remainder of Section 8, it will expire, renew and terminate in accordance with the terms of the Channel Partner Sale Agreement.

13.4. Fees and Payment. If Customer ordered the Subscription Services through a Channel Partner, then the provisions of Section 4 do not apply to Customer, and Customer's billing and payment rights and obligations are governed by the Channel Partner Sale Agreement. However, if the Channel Partner from whom Customer purchased the Subscription Services fails to pay Auth0 any amounts due in connection with Customer's use of the Subscription Services, then Auth0 may suspend Customer's rights to use the Subscription Services without liability, upon notice to Customer. Customer agrees that Customer's remedy in the event of such suspension is solely against the Channel Partner.

14. Miscellaneous Provisions

14.1. Affiliates. This Agreement set forth the general terms and conditions under which Auth0 will provide Subscription Services to Customer and its Affiliates.

14.2. Publicity; References. Auth0 may refer to Customer as one of Auth0's customers and use Customer's logo as part of such reference, provided that Auth0 complies with any trademark usage requirements notified to it by Customer.

14.3. Compliance With Laws. Each party will comply with all laws and regulations applicable to it, including U.S. export control laws. Neither party will have any liability to the other for any non-performance of their obligations under this Agreement to the extent that the non-performance is mandated by applicable law. Each party represents and warrants to the other that neither it nor its Affiliates, nor any of its or their users, officers or directors, are persons, entities or organizations with whom the other party is prohibited from dealing (including provision of

software, products or services) by virtue of any applicable law, regulation, or executive order, including US export control laws, and names appearing on the U.S. Department of the Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List.

14.4. U.S. Government Rights In The Subscription Services. Auth0 provides the Subscription Services for ultimate federal government end use solely in accordance with the following: Government technical data and software rights related to the Subscription Services include only those rights customarily provided to the public as defined in this Agreement. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data – Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a need for rights not conveyed under these terms, it must negotiate with Auth0 to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement.

14.5. Equitable Relief. Each of Customer and Auth0 acknowledges that damages will be an inadequate remedy if the other violates the terms of this Agreement pertaining to protection of a party's Intellectual Property Rights, Confidential Information or Personal Data. Accordingly, each of them will have the right, in addition to any other rights each of them may have, to seek in any court of competent jurisdiction, temporary, preliminary and permanent injunctive relief to restrain any breach, threatened breach, or otherwise to specifically enforce any of the obligations in this Agreement.

14.6. Business Continuity / Disaster Recovery. During any period in which Customer is subscribed to the Subscription Services, Auth0 will comply with its then current applicable Business Continuity and Disaster Recovery Plans. Auth0 will test such plans at least once a year.

14.7. Force Majeure. If the performance of this Agreement is adversely restricted or if either party is unable to conform to any warranty or obligation by reason of any Force Majeure Event then, except with respect to obligations to pay any fees or expenses and to obligations under Section 14.6 above (Business Continuity / Disaster Recovery), the party affected, upon giving prompt written notice to the other party, will be excused from such performance on a day-to-day basis to the extent of such restriction (and the other party will likewise be excused from performance of its obligations on a day-to-day basis to the extent such party's obligations relate to the performance so restricted); provided, however, that the party so affected will use all commercially reasonable efforts to avoid or remove such causes of non-performance and both parties will proceed whenever such causes are removed or cease. "**Force Majeure Event**" means any failure or delay caused by or the result of causes beyond the reasonable control of a party or its service providers that could not have been avoided or corrected through the exercise of reasonable diligence, including natural catastrophe, internet access or related problems beyond the demarcation point of the party's or its applicable infrastructure provider's facilities, state-sponsored malware or state-sponsored cyber-attacks, terrorist actions, laws, orders, regulations, directions or actions of governmental authorities having jurisdiction over the subject matter hereof, or any civil or military authority, national emergency, insurrection, riot or war, or other similar occurrence. If a party fails to perform its obligations as a result of such restriction for a period of more than 30 days, then the other party may terminate the affected Subscription Services without liability.

14.8. Service Performance Analytics. Auth0 may use Customer's and its Users' Subscription Services usage history, statistics and telemetry ("Analytics Data") for Auth0's internal analytical purposes related to its provision of Services, including to (i) detect security incidents, and protect against malicious, deceptive, fraudulent, or illegal activity; (ii) to identify errors that impair existing functionality; and (iii) undertake internal research for technological development. Auth0 may make information derived from its analysis of Analytics Data publicly available on an aggregated and anonymized basis, provided that such information does not contain any Personal Data of Customer's Users or identify either Customer or any of its Users. For the sake of clarity, such aggregated and anonymized data is not Confidential Information of Customer.

14.9. Captions and Headings. The captions and headings are inserted in this Agreement for convenience only, and will not be deemed to limit or describe the scope or intent of any provision of this Agreement.

14.10. Severability; Invalidity. If any provision of this Agreement is held to be invalid, such invalidity will not render invalid the remainder of this Agreement or the remainder of which such invalid provision is a part. If any provision of this Agreement is so broad as to be held unenforceable, such provision will be interpreted to be only so broad as is enforceable.

14.11. Waiver. No waiver of or with respect to any provision of this Agreement, nor consent by a party to the breach of or departure from any provision of this Agreement, will in any event be binding on or effective against such party unless it be in writing and signed by such party, and then such waiver will be effective only in the specific instance and for the purpose for which given.

14.12. Third Party Beneficiaries. Except as expressly set forth in this Agreement, no provisions of this Agreement are intended nor will be interpreted to provide or create any third party beneficiary rights or any other rights of any kind in any other party. If the law governing this Agreement is English law, then a person who is not a party to this Agreement will not have any rights under the Contracts (Rights of Third Parties) Act 1999) to enforce any term of this Agreement. Notwithstanding the foregoing, Auth0's suppliers of products and services delivered hereunder will enjoy the same disclaimers of warranty, limitations on liability and similar exculpatory provisions with respect to such products and services as does Auth0.

14.13. Assignment. Customer may not assign any of its rights or obligations under this Agreement without the prior written consent of Auth0. Subject to the foregoing restriction on assignment, this Agreement will be binding upon, inure to the benefit of and be enforceable by the parties and their respective successors and assigns.

14.14. Notices. Auth0 will provide Customer with notices that affect Auth0's customers generally (e.g., notices that relate to modifications or updates to, or the availability or interoperability of the Auth0 Platform) via e-mail or the Auth0 Platform dashboard or account center. Auth0 will provide Customer with any legal notices by pre-paid first class mail, air courier or e-mail to the mailing or e-mail address Customer provided Auth0 on the applicable Sales Order, or during Customer's registration for the Subscription Services, or to a substitute, updated mailing or e-mail address that Customer has provided to Auth0 for these purposes. Customer is responsible for keeping its mailing and e-mail address current with Auth0. Except as otherwise specified in this Agreement, all notices to be given to Auth0 under this Agreement must be in writing and sent to Auth0's USA headquarters by prepaid first class mail or air courier at the address specified on the first page of this Agreement (or, if none, at https://auth0.com/), marked "Attention: Legal Department". Notices sent electronically will be deemed received within 1 business day of dispatch. Notices sent by prepaid first class mail will be deemed received within 5 business days of dispatch (however, notices sent by mail to addressees in a different country from that of the sender will be deemed received upon delivery). Notices sent by air courier, or personally delivered, will be deemed received upon delivery.

14.15. Governing Language. The governing language for this Agreement and its related transactions, for any notices or other documents transmitted or delivered under this Agreement, and for the negotiation and resolution of any dispute or other matter between the parties, will be the English language. If there is any conflict between the provisions of any notice or document and an English version of the notice or document (including this Agreement), the provisions of the English version will prevail. Customer waives any rights it may have under any law in any state or country to have the Agreement written in any language other than English. In transactions between the parties, a decimal point will be indicated by a period, and not by a comma.

14.16. Entire Agreement; Amendments. This Agreement constitutes and embodies the entire agreement and understanding between the parties with respect to the subject matter hereof and supersedes all prior or contemporaneous written, electronic or oral communications, representations, agreements or understandings between the parties with respect thereto. This Agreement may not be modified or amended except in a written document to which both parties have assented (subject to modifications made in accordance with the Auth0 Modification Policy Additional Terms of Service referenced in Section 12 above). With the exception of the Additional Terms of Service, any additional, supplementary or conflicting terms supplied by Customer (whether in hard copy or electronic form), including those contained on or within any purchase order or standard terms of purchase, are specifically and expressly rejected by Auth0. In the event of any conflict between the provisions of this Agreement and any Sales Order, the provisions of this Agreement will prevail.

Exhibit A

Additional Data Protection Provisions for GDPR

1. Additional Definitions

1.1 For the purposes of this Exhibit A, the following initially capitalized words are ascribed the following meanings:

(a) "**Adequate Country**" means a country or territory that is recognized under EU Data Protection Laws from time to time as providing adequate protection for personal data;

(b) "**Auth0 Group**" means Auth0 and any corporate entities which are from time to time under Common Control with Auth0;

(c) "**Customer Group**" means Customer and any corporate entities which are from time to time: (a) under Common Control with Customer; and (b) established and/or doing business in the European Economic Area or Switzerland;

(d) "**EU Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom, applicable to the Processing of Personal Data under the Main Agreement, including (where applicable) the GDPR;

(e) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data;

(f) "**Personal Data**" means all data which is defined and regulated as 'Personal Data' in the EU Data Protection Laws and which is provided by Customer to Auth0 or accessed, stored or otherwise Processed by Auth0 in connection with the Auth0 Services;

(g) "**Properties**" means the websites, apps, platforms, APIs or other online properties and services owned or operated by or on behalf of Customer and/or other members of Customer Group, or their respective clients, in connection with which Customer uses the Services; and

(h) "**Processing**", "**data controller**", "**data subject**", "**supervisory authority**" and "**data processor**" will have the meanings ascribed to them in the EU Data Protection Laws.

1.2 An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "Common Control" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

2. Status of the parties

2.1 The type of Personal Data Processed pursuant to this DPA and the subject matter, duration, nature and purpose of the Processing, and the categories of data subjects, are as specified below:

(a) The ***personal data comprises***: email addresses, phone numbers or IP addresses, depending on the authentication method selected by Customer, and such other personal data as Customer selects, or is required by Customer's selected identity providers (IdPs);

(b) The ***duration of the Processing*** will be: until expiration or termination of the Subscription Term ;

(c) The ***nature and purpose of the Processing*** will comprise the following: Auth0 provides a user authentication and user authorization platform, which Customer may use to develop and integrate the identity management aspects of its own applications. The Auth0 Platform is not an application in itself; the Customer will need to write its own code to enable interoperability between the Auth0 Platform and Customer applications, and to determine how to use the Auth0 Platform within the Customer's architecture. Auth0 is responsible only for the Auth0 Platform. Auth0 is not responsible

for the Customer's networks, systems or applications (collectively, "Customer Systems"), the means by which the Customer chooses to integrate the Auth0 Platform into the Customer Systems, or the security and data protection measures that the Customer applies to the Customer Systems. The Auth0 Platform acts as a broker for momentary transactions between users (i.e., data-subjects) and Customer applications. Auth0 has minimal control over the nature and scope of the personal data that Customer chooses to Process using the Auth0 Platform, minimal insight into the identity of the Customer's users, and no role in the Customer's decision-making as to the purpose for which the personal data is Processed.

(d) The ***purpose(s) of the Processing*** is / are: as necessary for the provision of the Subscription Services;

(e) ***Data subjects*** are end users, or individuals purporting to be end users, of Customer's Properties, or other data subjects with respect to whom Customer elects to collect their personal data, and Customer's and Customer Group members', and its and their service providers', employees, consultants, agents and representatives authorized by Customer to use the Services.

2.2 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties acknowledge and agree that Customer is the data controller and Auth0 is the data processor and accordingly Auth0 agrees that it will Process all Personal Data in accordance with its obligations pursuant to this Exhibit A.

2.3 Each of Auth0 and Customer will notify to each other one or more individuals within its organisation authorised to respond from time to time to enquiries regarding the Personal Data and each of Auth0 and Customer will deal with such enquiries promptly.

3. **Auth0 obligations**

3.1 With respect to all Personal Data, Auth0 agrees that it will:

(a) Insofar as required under GDPR, comply with its obligations with respect to its Processing of Personal Data under Sections 7.2-7.9 of the main body of the Agreement (Instructions; Information Security; Audits and Security Assessments; Data Export, Retention and Destruction; Sub-Processors; Access by Auth0 Personnel; User Requests; Breach Notification);

(b) in the unlikely event that applicable law requires Auth0 to Process Personal Data other than pursuant to Customer's instructions, Auth0 will notify Customer (unless prohibited from so doing by applicable law);

(c) as soon as reasonably practicable upon becoming aware, inform Customer if, in Auth0's opinion, any instructions provided by Customer under Section 7.2 of the main body of the Agreement violate the GDPR;

(d) as more particularly described in Section 7.3 of the main body of the Agreement, implement appropriate technical and organisational measures designed to ensure a level of security appropriate to the risks that are presented by the Processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data in Auth0's possession or under its control. Such measures include the security measures specified in Exhibit A-1 below.

(j) taking into account the nature of Processing and the information available to Auth0, assist Customer when reasonably requested in relation to Customer's obligations under EU Data Protection Laws with respect to:

(i) data protection impact assessments (as such term is defined in the GDPR);

(ii) notifications to the supervisory authority under EU Data Protection Laws and/or communications to data subjects by Customer in response to any Security Breach; and

(iii) Customer's compliance with its obligations under the GDPR with respect to the security of Processing.

(k) taking into account the nature of the Processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, to respond to data subjects' requests to exercise their rights under Chapter III of the GDPR. Auth0 will promptly notify Customer of requests received by Auth0, unless otherwise required by applicable law. Customer may make changes to Personal Data Processed with the Auth0 Platform using the features and functionality of the Auth0 Platform. Auth0 will not make changes to such data except as agreed in writing with Customer.

4. **Data transfers**

4.1 To the extent any Processing of Personal Data by Auth0 takes place in any country outside the EEA (other than exclusively in an Adequate Country), the parties agree that the standard contractual clauses approved by the EU authorities under EU Data Protection Laws ("SCCs") will apply in respect of that Processing and Auth0 will comply with the obligations of the 'data importer' in the standard contractual clauses and Customer will comply with the obligations of 'data exporter'. The security measures applicable to the SCCs are those specified in Exhibit A-1 to this Exhibit A.

4.2 If, in the performance of this Agreement, Auth0 transfers any Personal Data to a sub-processor (or any member of the Auth0 Group that acts as a sub-processor) other than exclusively in an Adequate Country, Auth0 will in advance of any such transfer ensure that a mechanism to achieve adequacy in respect of that Processing is in place such as:

(a) the requirement for Auth0 to execute or procure that the third party execute on behalf of Customer standard contractual clauses approved by the EU authorities under EU data Protection Laws;

(b) the requirement for the third party to be certified under the Privacy Shield framework; or

(c) the existence of any other specifically approved safeguard for data transfers (as recognised under the EU Data Protection Laws) and/or a European Commission finding of adequacy.

4.3 The following terms will apply to the standard contractual clauses:

(a) The Customer may exercise its right of audit under clause 5.1(f) of the standard contractual clauses as set out in, and subject to the requirements of, Section 7.4 of the main body of the Agreement; and

(b) The data importer may appoint sub-processors as set out, and subject to the requirements of, Section 7.6 of the main body of the Agreement.

Exhibit A-1

Security Measures

As used in this Exhibit A-1, "Data Importer" refers to the data processor, and "Data Exporter" refers to the data controller.

The Data Importer currently abides by the security standards in this Exhibit 3. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a degradation of the overall security of the Services during the term of the applicable Services Agreement.

Hosting Infrastructure. Infrastructure. The Data Importer hosts its services in geographically distributed, secure data centers operated by Amazon Web Services (AWS). Redundancy. The services are replicated across multiple data centers within a geographic region to eliminate single points of failure using an active/passive configuration in order to minimize the impact of environmental risks. Monitoring. The services are protected by automated monitoring which is designed to detect a variety of failure conditions and which will, when appropriate, trigger failover mechanisms. Backups. Backups are performed on a regular basis and stored in a secondary site within the same geographic region. Business Continuity. The Data Importer replicates its service and data over multiple data centers within a geographic region to protect against loss of service or data. The Data Importer conducts periodic tests of failover and data backup procedures to ensure readiness for business continuity and disaster recovery.

Networks & Transmission. Network Data Transmission. Interactions between users, administrators and Data Importer modules are done using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) standard cryptographic protocols. Network Security. The Data Importer employs multiple layers of DOS protection, Intrusion Detection, Rate Limiting and other network security services from both its hosting providers and third party providers. Encryption Technologies. The Data Importer makes HTTPS encryption (also referred to as SSL or TLS connection) available.

Policies and Procedures. Policies. The Data Importer has written, approved policies governing Account Management, Acceptable Use, Data Retention, Employee Code of Conduct, Encryption, Incident Response, Information Sensitivity, Use of Mobile Devices, Password Protection, Patch Management and Risk Management. Procedures. The Data Importer has written and approved procedures for Data Breach Notification, Change Management, Communication, Disaster Recovery, DoS Response, System Backup and Recovery, and Monitoring. Security Response. The Data Importer monitors a variety of communication channels for security incidents, and the Data Importer's security personnel are required to react promptly to known incidents.

Access Controls. Access Procedures. The Data Importer maintains formal access procedures for allowing its personnel access to the production service and components involved in building the production service. Only authorized employees are allowed access to these restricted components and all access is approved by an employee's manager and service owner. Only a small number of individuals are approved to access the restricted components. Audit records are maintained to indicate who has access to restricted components. Access Mechanisms. Access to the Data Importer's production service and build infrastructure occurs only over a secured channel and requires two-factor authentication. Logging. Access to the Data Importer's production service and build infrastructure is done using unique IDs and is logged. Infrastructure Security Personnel. The Data Importer maintains several security policies governing its personnel. The Data Importer's infrastructure security personnel are responsible for the ongoing monitoring of the Data Importer's security infrastructure, the review of the Services, and responding to security incidents.

Data Protection. In Transit. Interactions between users, administrators and Auth0 modules are done using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) standard cryptographic protocols. At Rest. The Data Importer uses cryptographic hashing and encryption mechanisms to protect sensitive information such as cryptographic keys and application secrets. Redundancy. The Data Importer stores data in a multi-tenant environment within the Data Importer's hosted infrastructure. The data and service are replicated across multiple hosted datacenters within the same geographic region. Data Isolation. The Data Importer logically isolates the Data Exporter's data, and the Data Exporter has a large degree of control over the specific data stored in the Service. Data

Deletion. The Data Importer provides to the Data Exporter a mechanism that can be used to delete the Data Exporter's data.

Software Code Review. The Data Importer employs a code review process to improve the security of the code used to provide the Services. All changes to the service are reviewed and approved by a senior engineer other than the author of the change. Automated testing. Each software build is subjected to a comprehensive suite of automated tests. Security Scan. The Data Importer employs a third party to scan the Service for security vulnerabilities on a periodic basis.

Staff Conduct and Security. Staff Conduct. The Data Importer personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, usage, compliance and professional standards. Background Checks. The Data Importer conducts reasonably appropriate backgrounds checks as legally permissible and in accordance with applicable local labor law and statutory regulations.

Sub-processor Security. Prior to onboarding sub-processors that will handle any data provided by a Data Exporter, the Data Importer conducts an assessment of the security and privacy practices of the sub-processor to help ensure that the sub-processor provides a level of security and data protection controls appropriate to their access to data and the scope of the services they are engaged to provide.

Data Privacy Office. The Data Privacy Office of the Data Importer can be contacted by the Data Exporter's administrators using the mechanism defined at: https://auth0.com/privacy (or via such other means as may be provided by the Data Importer).

.