



AUTH0, INC.

DATA PROCESSING ADDENDUM (Pre-Signed by Auth0)

INSTRUCTIONS FOR EXECUTING THIS DATA PROCESING ADDENDUM

This Data Processing Addendum (“DPA”), including if applicable the Controller-Processor Standard Contractual Clauses in Exhibit 2, has been pre-signed on behalf of Auth0, Inc. To complete and execute this document, Customer must:

1. Complete the information for the Customer signature box on Page 1;
2. Complete the information as the data exporter on page 14 and page 17; and
3. Email the completed and signed DPA to legal-scc@auth0.com.

If Customer does not already have a DPA with Auth0, this DPA will become legally binding upon the later to occur of the “Effective Date” (defined below) of the DPA or Auth0’s receipt of a completed and fully executed DPA at the email address specified above.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement (defined below), this DPA is an addendum to and forms part of the Agreement. In such case, the Auth0 entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed a Sales Order with Auth0 pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Sales Order and applicable renewal Sales Orders.

If the entity signing this DPA as a “Customer” is neither a party to a Sales Order nor the Agreement, then this DPA is not valid and is not legally binding. Auth0 recommends that the entity should request that the Customer entity that is a party to the Agreement executes this DPA.


**AUTH0, INC.
DATA PROCESSING ADDENDUM**

THIS DATA PROCESSING ADDENDUM (“DPA”) is made between Auth0, Inc. (“Auth0”), a Delaware, USA corporation whose principal offices are at 10800 NE 8th Street, Suite 700, Bellevue, WA 98004, U.S.A., and the Customer identified below. This DPA is incorporated into and made subject to the Identity Management Platform Subscription Agreement between Auth0 and Customer, or to any other written agreement between Auth0 and Customer (such as Auth0’s Free, Developer and Developer Pro Terms of Service), that governs Customer’s use of the Services (as defined below) (the “**Agreement**”).

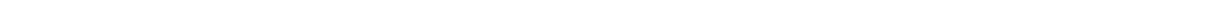
BACKGROUND

- (A) Auth0 provides an identity management platform-as-a-service solution (“**Services**”) to Customer under the Agreement. In connection with the Services, Auth0 processes certain personal data in respect of which Customer or any Customer Affiliate (as defined below), or customers of Customer or its Affiliates, may be a data controller under the Data Protection Laws (as defined below).
- (B) Customer and Auth0 have agreed to enter into this DPA in order to establish their respective responsibilities under the Data Protection Laws.
- (C) All capitalized terms used in this DPA but not otherwise defined have the meaning ascribed to them in the Agreement.

EXECUTED as of the date set forth below Customer’s signature (the “**Effective Date**”):

AUTH0, INC.
 By: 
 (Name): Preston Graham
 Title: VP of Finance
 Date: 8/21/2020

CUSTOMER
 Company Name:
 By (Signature):
 Printed Name:
 Title:
 Date:



1. Definitions

- 1.1 For purposes of this DPA, the following initially capitalized words have the following meanings:
- (a) “**Adequate Country**” means a country or territory that is recognized under applicable Data Protection Laws from time to time as providing adequate protection for personal data.
 - (b) “**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.

- (c) **“Auth0 Platform”** means the computer software applications, tools, application programming interfaces (APIs), and connectors provided by Auth0 as its online identity management platform as a service offering, together with the programs, networks and equipment that Auth0 uses to make such platform available to its customers.
- (d) **“Authorized Affiliate”** means any of Customer’s Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area, their member states, Switzerland, and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Auth0, but has not signed its own Sales Order with Auth0 and is not a “Customer” as defined under this DPA.
- (e) **“Customer”** means the entity that executed the Agreement, together with its Affiliates (for so long as they remain Affiliates) that have signed Sales Orders with Auth0.
- (f) **“Customer Data”** means any data that Customer or its Users input into the Auth0 Platform for Processing as part of the Services, including any Personal Data forming part of such data.
- (g) **“Data Protection Laws”** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states, Switzerland, and/or the United Kingdom, applicable to the processing of Personal Data under the Agreement, including (where applicable) the GDPR.
- (h) **“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 (known as the General Data Protection Regulation).
- (i) **“Personal Data”** means Customer Data consisting of any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws).
- (j) **“Standard Contractual Clauses”** or (**“SCCs”**) means the standard contractual clauses approved by the European Commission for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.
- (k) **“processing”, “data controller”, “data subject”, “supervisory authority”** and **“data processor”** have the meanings ascribed to them in the GDPR.

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 described in Exhibit 1.
- 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. Auth0 agrees that it will process all Personal Data in accordance with its obligations pursuant to this DPA.
- 2.3 As between the parties, Customer is solely responsible for obtaining, and has obtained or will obtain, all necessary consents, licenses and approvals for the processing, or otherwise has a valid legal basis under Data Protection Laws for the Processing of Personal Data (the “Customer Legal Basis Assurance”). Without limiting the Customer Legal Basis Assurance, each of Customer and Auth0 warrant in relation to Personal Data that it will comply with (and will ensure that any of its personnel comply with), the Data Protection Laws applicable to it.

3. **Auth0 obligations**

- 3.1 Instructions. Auth0 will only process the Personal Data in order to provide the Services and will act only in accordance with the Agreement and Customer's written instructions. The Agreement, this DPA, and Customer's use of the Auth0 Platform's features and functionality, are Customer's written instructions to Auth0 in relation to the processing of Personal Data.
- 3.2 Contrary Laws. If the Data Protection Laws require Auth0 to process Personal Data other than pursuant to Customer's instructions, Auth0 will notify Customer prior to processing (unless prohibited from so doing by applicable law).
- 3.3 Infringing Instructions. Auth0 will immediately inform Customer if, in Auth0's opinion, any instructions provided by Customer under Clause 3.1 infringe the GDPR or other applicable Data Protection Laws.
- 3.4 Appropriate Technical and Organizational Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, Auth0 will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing, in particular from 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 security measures equal to or better than those specified in Exhibit 3 below. Customer has reviewed Auth0's security program and acknowledges that it is designed to ensure a level of security appropriate to the risk. Customer further acknowledges that it is responsible for its configuration of the Auth0 Platform and for using features and functionality of the Services to ensure a level of security appropriate to the risks presented by the processing.
- 3.5 Access by Auth0 Personnel. Auth0 will ensure that its personnel have access to Personal Data only as necessary to perform the Services in accordance with the Agreement and this DPA, and that any persons whom it authorises to have access to the Personal Data are under written obligations of confidentiality.
- 3.6 Personal Data Breaches. Taking into account the nature of the processing and the information available to Auth0:
- (a) Auth0 will, without undue delay after becoming aware, notify Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Auth0's possession or under its control (including when transmitted, stored or otherwise processed by Auth0) (a "**Personal Data Breach**");
 - (b) Auth0 will promptly provide Customer with reasonable cooperation and assistance in respect of the Personal Data Breach and information in Auth0's possession concerning the Personal Data Breach, including, to the extent then-known to Auth0, the following:
 - (i) the nature of the Personal Data Breach;
 - (ii) the categories and approximate number of data subjects concerned;
 - (iii) the categories and approximate number of Personal Data records concerned;
 - (iv) the likely consequences of the Personal Data Breach;
 - (v) a summary of the unauthorised recipients of the Personal Data; and

- (vi) the measures taken or proposed to be taken by Auth0 to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;
- (c) Insofar as a Personal Data Breach relates to Customer, Auth0 will not make any announcement about a Personal Data Breach (a “**Breach Notice**”) without:
 - (i) the prior written consent from Customer; and
 - (ii) prior written approval by Customer of the content, media and timing of the Breach Notice;

unless required to make a disclosure or announcement by applicable law.

3.7 Deletion or Return of Personal Data. Auth0 will return Personal Data to Customer by permitting Customer to export Personal Data from the Auth0 Platform at any time during provision of the Services, using the Auth0 Platform’s then existing features and functionality. Customer may delete Customer Data on its “Tenants” at any time. (“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.) 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 Personal Data retained by Auth0 (if any). Auth0 is not obligated to delete copies of Personal Data retained in automated backup copies generated by Auth0, which Auth0 will retain for up to, and delete within, 14 months from their creation. Such backup copies will remain subject to this DPA and the Agreement until they are destroyed.

3.8 Assistance. Taking into account the nature of processing and the information available to Auth0, Auth0 will assist Customer when reasonably requested in relation to Customer’s obligations under 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 Data Protection Laws and/or communications to data subjects by Customer in response to any Personal Data Breach; and
- (iii) prior consultations with supervisory authorities.

3.9 Data Subject Requests. Taking into account the nature of the processing, Auth0 will 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. If and to the extent that Customer is unable to respond to a data subject request by using features and functionality of the Auth0 Platform and a response to the data subject is required by Data Protection Laws, Auth0 will, upon written request by Customer, reasonably assist Customer in responding to the request.

3.10 Records of Processing Activities. Auth0 will maintain records of its processing activities as required by Article 30.2 of the GDPR, and make such records available to the applicable supervisory authority upon request.

4. **Sub-processing**

- 4.1 **Disclosure and Transfer of Personal Data.** Auth0 will not disclose or transfer Personal Data to any third party without the prior written permission of Customer, except (i) as specifically stated in the Agreement or this DPA, or (ii) where such disclosure or transfer is required by any applicable law, regulation, or public authority.
- 4.2 **Consent to Sub-Processors.** Customer consents to Auth0's use of sub-processors to provide aspects of the Services, and to Auth0's disclosure and provision of Personal 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 Personal 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.
- 4.3 **Authorization of New Sub-Processors.** Auth0 may authorize new sub-processors, provided that:
- (a) Auth0 provides at least 30 days prior written notice to Customer of the authorization of any new sub-processor to process Personal Data in connection with its provision of Services (including details of the processing and location) and Auth0 will update the list of all sub-processors engaged to process Personal Data under this DPA published at <https://auth0.com/legal> and make such updated version available to Customer prior to such authorization of the sub-processor;
 - (b) Auth0 requires each sub-processor Auth0 so authorizes to comply with terms which are substantially no less protective of Personal Data than those imposed on Auth0 in this DPA, to the extent reasonably applicable to the services such sub-processor provides; and
 - (c) Auth0 remains liable for any breach of its obligations under this DPA that is caused by an act, error or omission of the sub-processor.
- 4.4 **Objections to New Sub-Processors.** 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 Personal Data by the objected to sub-processor within a reasonable period of time, not to exceed 30 days from receipt of the objection (the "Correction Period"), then, at any time within expiration of the Correction Period, Customer may elect to terminate the processing of Personal Data under affected Sales Orders to the Agreement without penalty, by written notice to Auth0 to that effect. If Customer terminates any such Sales Order in accordance with the foregoing, then Auth0 will refund to Customer a pro-rata amount of any affected Services fees prepaid to Auth0 and applicable to the unutilized portion of the Subscription Term for terminated Services.

5. **Audit and records**

- 5.1 **Provision of Information.** Auth0 will make available to Customer such information in Auth0's possession or control as Customer may reasonably request with a view to demonstrating Auth0's compliance with the obligations of data processors under the Data Protection Laws in relation to its processing of Personal Data.
- 5.2 **Audit Right.** Customer may exercise its right of audit under the Data Protection Laws, through Auth0 providing:

- (a) an audit report or certification not older than 12 months by an independent external auditor demonstrating that Auth0's technical and organizational measures are in accordance with Auth0's SOC-2 Statement and the ISO 27001 and ISO 27018 standards; and
- (b) additional information in Auth0's possession or control to an EU supervisory authority when it requests or requires additional information in relation to the data processing activities carried out by Auth0 under this DPA.

6. Data transfers

This Section 6 applies to any processing by Auth0 or its sub-processors of any Personal Data subject to the GDPR.

- 6.1 To the extent any processing by Auth0 of Personal Data takes place in any country outside the European Economic Area ("EEA") (other than exclusively in an Adequate Country), the parties agree that the Standard Contractual Clauses will apply in respect of that processing; 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'. In this respect, Customer and Auth0 have each executed Standard Contractual Clauses, attached as Exhibit 2, which are incorporated into and made subject to this DPA by this reference.
- 6.2 Customer acknowledges that the provision of the Services under the Agreement may require the processing of Personal Data by sub-processors in countries outside the EEA from time to time.
- 6.3 If, in the performance of this DPA, Auth0 transfers any Personal Data to a sub-processor (including any Auth0 Affiliate that acts as a sub-processor) where such sub-processor will process Personal Data outside the EEA (other than exclusively in an Adequate Country), then 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 Standard Contractual Clauses;
 - or
 - (b) any other specifically approved safeguard for data transfers (as recognised under the Data Protection Laws) and/or a European Commission finding of adequacy.
- 6.4 The following terms will apply to the Standard Contractual Clauses (whether used pursuant to Section 6.1 or 6.3(a) of this DPA):
 - (a) The Standard Contractual Clauses apply to (i) a Customer which is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom and, (ii) its Authorized Affiliates. For the purpose of the Standard Contractual Clauses, such entities constitute "data exporters".
 - (b) For the purposes of clause 5(a) of the Standard Contractual Clauses, the Agreement, this DPA, and Customer's use of the Auth0 Platform's features and functionality, are Customer's written instructions to Auth0 in relation to the processing of Personal Data.
 - (c) Customer's right of audit under clauses 5(f) and 12.2 of the Standard Contractual Clauses may be exercised as specified in Section 5.2 of this DPA.
 - (d) Pursuant to clause 5(h) of the Standard Contractual Clauses, Auth0's Affiliates may be retained as sub-processors, and Auth0 and its Affiliates respectively may engage third-party sub-processors in connection with the provision of the Services. Auth0 will make available its then-

current list of sub-processors available to Customer in accordance with Section 4.2 of this DPA. Pursuant to clause 5(h) of the Standard Contractual Clauses, Auth0 may engage new sub-processors as described in Sections 4.3 and 4.4 of this DPA. The parties agree that copies of sub-processor agreements that Auth0 must provide to Customer pursuant to clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Auth0 beforehand; and, that such copies will be provided by Auth0 only upon request by Customer.

- (e) For purposes of clause 12.1 of the Standard Contractual Clauses, Auth0 will (a) comply with its obligations to return or destroy all Personal Data as specified in Section 3.7 of this DPA, and (b) provide certification of its destruction of such data only upon Customer's written request.

7. Authorized Affiliates

7.1 By executing the Agreement, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Auth0 and each such Authorized Affiliate, subject to the provisions of the Agreement and this Section 7 and Section 8. Each Authorized Affiliate agrees to be bound by the obligations of Customer under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA.

7.2 The Customer that is the contracting party to the Agreement will remain responsible for coordinating all communication with Auth0 under this DPA and will be entitled to make and will receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

7.3 Where an Authorized Affiliate becomes a party to the DPA with Auth0 it will, to the extent required under applicable Data Protection Laws, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

- (a) Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Auth0 directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement will exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in Section 7.3(b) below).
- (b) The Customer that is the contracting party to the Agreement will, when carrying out any audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Auth0 and its sub-processors by combining, to the extent reasonably possible, several audit requests of itself and all of its Authorized Affiliates in one single audit.

8. Limitation of Liability

8.1 Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Auth0, whether in contract, tort or under any other theory of liability, is subject to the 'Limitations and Exclusions of Liability' (or its equivalent) section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Auth0's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs will apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, will not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

9. **General**

- 9.1 This DPA is without prejudice to the rights and obligations of the parties under the Agreement which will continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA will prevail insofar as the subject matter concerns the processing of Personal Data. In the event of any conflict between the terms of this DPA and the Standard Contractual Clauses then, only insofar as the Standard Contractual Clauses apply, the Standard Contractual Clauses will prevail.
- 9.2 Customer and Auth0 each agree that the dispute resolution provisions of the Agreement (including governing law and venue) apply to this DPA.

Exhibit 1

Details of the Personal Data and processing activities

- (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 Agreement;
- (c) 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 means by which Customer obtains personal data of Customer's users or 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 Services;
- (e) data subjects are end users, or individuals purporting to be end users, of the Customer Applications, or other data subjects with respect to whom Customer elects to collect their personal data, and Customer's and Customer Affiliate members', and its and their service providers, employees, consultants, agents and representatives authorized by Customer to use the Services.

Exhibit 2

2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

INTRODUCTION

Both parties have agreed on the following Contractual Clauses (the “**Clauses**”) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

AGREED TERMS

1. Definitions

For the purposes of the Clauses:

- (a) “**personal data**”, “**special categories of data**”, “**process/processing**”, “**controller**”, “**processor**”, “**data subject**” and “**supervisory authority**” shall have the same meaning as in Data Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) the “**data exporter**” means the entity who transfers the personal data;
- (c) the “**data importer**” means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) the “**sub-processor**” means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) the “**applicable data protection law**” means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; and
- (f) “**technical and organisational security measures**” means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

- 3.1 The data subject can enforce against the data exporter this Clause, Clause 4.1(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- 3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data

exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

- 3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

- (j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

- 6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

- 6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

- 6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

- 7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

- 7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Co-operation with supervisory authorities

- 8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
- 8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
- 8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. Governing law

The Clauses shall be governed by the governing law of the member state in which the data exporter is established, namely the member state in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Sub-processing

- 11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor’s obligations under such agreement.
- 11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the member state in which the data exporter is established.
- 11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.1(j), which shall be updated at least once a year. The list shall be available to the data exporter’s data protection supervisory authority.

12. Obligation after the termination of personal data-processing services

- 12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
- 12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

This agreement has been entered into on the date shown at the beginning of the first page of this agreement.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature

On behalf of the data importer:

Name (written out in full): Preston Graham

Position: VP of Finance

Address:

Other information necessary in order for the contract to be binding (if any):

Signature 
07A898B529EC46C...

Appendix 1
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

An entity that has subscribed to the data importer's online user authentication and user management platform-as-a-service solution.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

A US company providing an online user authentication and user management platform-as-a-service solution in relation to users of websites, apps and other online properties.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

End users, or those purporting to be end users, of the data exporter's websites, apps or other online properties, or other data subjects with respect to whom Customer elects to collect their personal data, and the data exporter's, its affiliates, and its and their service providers', employees, consultants, agents and representatives authorized by data exporter to use the data importer's services.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Email addresses, phone numbers or IP addresses, depending on the authentication method selected by data exporter, and such other personal data as data exporter selects, or is required by Customer's selected identity providers (IdPs).

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Such categories of data as data exporter selects.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Storage and analysis of user login and related data for the purposes of user authentication and user authorization.

DATA EXPORTER


Name:

Authorised Signature

DATA IMPORTER

Preston Graham

Name: DocuSigned by:.....


07A898B529EC48C...

Authorised Signature

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The Data Importer currently abides by the security standards in this Appendix 2. 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 (when made available by Data Importers infrastructure as a service providers) 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.

Subprocessor 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).

Exhibit 3 to the DPA

Security Measures

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).