INTERNATIONAL DATA PROCESSING ADDENDUM TO THE SUBSCRIPTION AGREEMENT

This International Data Processing Addendum (this "**DPA**") to the Subscription Agreement between Auth0 and Customer (the "**Main Agreement**") contains terms to ensure that adequate safeguards are in place with respect to the protection of personal data to be processed by Auth0 pursuant to the Main Agreement, as required by the EU Data Protection Laws. By indicating Customer's acceptance of this DPA, or by executing a "**Sales Order**" under the Main Agreement that references this DPA, Customer agrees to be bound by this DPA. If you are entering into this DPA 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 DPA. If you do not have that authority or if Customer does not agree with the terms of this DPA, then you may not indicate acceptance of this Agreement. The "**Effective Date**" of this DPA is the date on which you first indicate your assent to the terms of this Agreement.

THIS DATA PROCESSING ADDENDUM is made as of the Effective Date, between Customer and Auth0.

RECITALS

(A) Auth0 provides a user authentication and user authorization platform-as-a-service solution ("**Auth0 Services**") to Customer under the Main Agreement. In connection with the Auth0 Services, Auth0 processes certain personal data in respect of which Customer or any member of Customer Group (as defined below), or clients of Customer or a member of Customer Group, may be a data controller under the EU Data Protection Laws (as defined below).

(B) The Customer and Auth0 have agreed to enter into this addendum ("**DPA**") in order to ensure that adequate safeguards are put in place with respect to the protection of such personal data as required by the EU Data Protection Laws.

Definitions

1.1 The following expressions are used in this DPA:

(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. During any period in which Auth0 is certified under the EU-US Privacy Shield Program, the USA will be treated as an Adequate Country for purposes of this DPA;

(b) **"Auth0"** means Auth0, Inc., a Delaware corporation whose principal place of business is at 10900 NE 8th Street, Suite 700, Bellevue, WA 98004, USA.

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

(d) **"Auth0 Costs**" means all reasonable costs and expenses, including compensation for provision of human resources at Auth0's (and, if applicable, any affected sub-processors') then current professional services rates.

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

(f) **"Customer"** means the entity identified as such in the Main Agreement or the applicable Sales Order.

(g) "**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;

(h) "**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;

(i) "**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)

(j) "**Personal Data**" means all data which is defined 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;

(k) "**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

(l) "**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.

1.3 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; and (iv) "will" is, unless the context requires otherwise, an expression of command, not merely an expression of future intent or expectation..

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 As between the parties, Customer is solely responsible for obtaining, and represents and covenants that it has obtained and will obtain, all necessary consents, licenses and approvals for the processing of any Personal Data as part of the Services (the "Customer Consent Assurance"). Each of Customer and Auth0 warrant in relation to Personal Data that it will comply with (and will ensure that any of its staff and/or subcontractors comply with), the EU Data Protection Laws; provided, however, that Auth0's warranty is subject to Customer Consent Assurance.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby 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 DPA.

2.4 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 warrants that it will:

(a) only process the Personal Data in order to provide the Services and will act only in accordance with this Agreement and Customer's written instructions. This Agreement, and Customer's use of the Auth0 Platform's features and functionality, are Customer's initial set of instructions to Auth0 in relation to the processing of personal data. Customer may issue supplemental instructions that are consistent with the terms of the Subscription Agreement and the Auth0 Platform. If any supplemental instruction requires activity by Auth0 outside the scope of the Services, then Customer will bear and pay all Auth0 Costs;

(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 Clause 3.1(a) infringe the GDPR;

(d) implement appropriate technical and organisational measures 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 3 below.

(e) take reasonable steps to ensure that only authorised personnel have access to such Personal Data and that any persons whom it authorises to have access to the Personal Data are under obligations of confidentiality;

(f) as soon as reasonably practicable upon becoming aware, notify Customer of any actual or alleged incident of unauthorised or accidental disclosure of or access to any Personal Data by any of its staff, sub-processors or any other identified or unidentified third party (a "**Security Breach**");

(g) promptly provide Customer with reasonable cooperation and assistance in respect of the Security Breach and all information in Auth0's possession concerning the Security Breach, including, to the extent known to Auth0, the following:

(i) the possible cause and consequences of the Security Breach;

(ii) the categories of Personal Data involved (Customer acknowledges that since Customer selects the Personal Data processed with the Auth0 Platform, and since Auth0 does not typically have visibility into the scope and nature of such Personal Data, Customer is responsible for determining such categories);

(iii) a summary of the possible consequences for the relevant data subjects (Customer acknowledges that since Customer selects the Personal Data processed with the Auth0 Platform as described above, and the data subject to whom such personal data relates, and since Auth0 does not typically have visibility into the foregoing, Customer is primarily responsible for determining such consequences);

(iv) a summary of the unauthorised recipients of the Personal Data; and

(v) the measures taken by Auth0 to mitigate any damage;

(h) insofar as a Security Breach relates to Customer, not make any announcement about a Security 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.

(i) Customer may export Personal 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 Personal Data. On Customer's request or otherwise on following termination of the Subscription Services, if and to the extent Customer cannot delete or overwrite Personal Data stored on Auth0's systems using the then existing features and functionality of the Auth0 Platform, Auth0 will destroy Personal Data in Auth0's custody or control. Auth0 will regularly dispose of Personal Information that is maintained by Auth0 separate from the Auth0 Platform ("Incidental Data"), but that is no longer necessary to provide the Subscription Services. Auth0's obligations to destroy Personal Data and Incidental Data are subject to Auth0's customary backup and archival processes; backup and archival copies of data will remain subject to this Agreement until they are destroyed. Customer will bear and pay for all Auth0 Costs related to any destruction of Personal Data or Incidental Data that Customer requires Auth0 to perform that is outside the scope of Auth0's customary destruction processes.

(j) provide such assistance as Customer reasonably requests (taking into account the nature of processing and the information available to Auth0) to the Client in relation to the Client'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;

provided Customer will bear and pay for all Auth0 Costs related to provision of the assistance in this clause 3.1(j).

4. **Sub-processing**

4.1 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 this Agreement, or (ii) where such disclosure or transfer is required by any applicable law, regulation, or public authority.

4.2 For these purposes Customer consents to the disclosure of Personal Data to members of the Auth0 Group that act as sub-processors. Customer further consents to the disclosure of Personal Data to other sub-processors whom Auth0 uses to provide the Subscription Services (a list of current sub-processors is published at https://auth0.com/legal); 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 Agreement 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 Agreement, 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 Agreement that is caused by an act, error or omission of a sub-processor.

4.3 If Customer objects to the authorization of any future sub-processor on reasonable data protection grounds within 10 business 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, then, at any time within expiration of such 30 days period, Customer may elect to terminate the processing of Personal Data under this Agreement without penalty, by notice to Auth0 to that effect. If Customer terminates the Services 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 Auth0 will, in accordance with EU Data Protection Laws, 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 EU Data Protection Law in relation to its processing of Personal Data.

5.2 The Customer may exercise its right of audit under EU Data Protection Laws, through Auth0 providing:

(a) an audit report not older than 18 months by an independent external auditor demonstrating that Auth0's technical and organizational measures are in accordance with Auth0's SOC-2 Statement or similar accepted industry audit standard; 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

6.1 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 and set out in Exhibit 2 (the "**SCCs**") will apply in respect of that processing and Auth0 will comply with the obligations of the 'data importer' in the SCCs and Customer will comply with the obligations of 'data exporter'. If and to the extent that the SCCs apply, signatures or another effective indication of assent of Auth0 and Customer to a Sales Order that references this DPA will be deemed signatures to the SCCs and each appendix to the SCCs.

6.2 The Customer acknowledges that the provision of the Services under the Main 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 (or any member of the Auth0 Group that acts as a sub-processor) and without prejudice to clause 4 where such sub-processor will process Personal Data outside the EEA (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 and set out in Exhibit 2;

(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.

6.4 The following terms will apply to the standard contractual clauses set out in Exhibit 2 (whether used pursuant to clause 6.1 or 6.3(a)):

(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, clause 5.2 of this DPA; and

(b) The data importer may appoint sub-processors as set out, and subject to the requirements of, clauses 4 and 6.3 of this DPA.

7. **General**

7.1 This DPA is without prejudice to the rights and obligations of the parties under the Main 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 Main Agreement, the terms of this DPA will prevail so far as the subject matter concerns the processing of Personal Data.

7.2 Auth0's maximum aggregate liability to Customer and to each member of Customer Group (taken together) under or in connection with this DPA (including under the standard contractual clauses set out in Exhibit 3) will not under any circumstances exceed the applicable maximum aggregate liability of Auth0 to Customer as specified in the Main Agreement. Nothing in this Addendum will limit Auth0's liability in respect of bodily injury or death in negligence or for any other liability or loss which may not be limited by agreement under applicable law.

7.3 This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. Other than in respect of statements made fraudulently, no other representations or terms will apply or form part of this DPA.

7.4 A person who is not a party to this DPA will not have any rights under this DPA (including under the Contracts (Rights of Third Parties) Act 1999) to enforce any term of this DPA.

7.5 This DAP will be governed by and interpreted in accordance with the internal laws of the State of Washington and, where such laws are pre-empted by the laws of the United States, by the internal laws of the United States, without regard to conflicts of laws principles. In the event of any controversy or claim arising out of or relating to this Agreement, or the breach or interpretation thereof, the parties will submit to the exclusive jurisdiction of and venue in the State courts of Washington located in Seattle, or the Federal District Court for the Western District of Washington, and appeal courts therefrom. Each party hereby waives all defenses of lack of personal jurisdiction and forum nonconveniens. Process may be served on either party in the manner authorized by applicable law or court rule. If any proceeding is brought by either party to enforce or interpret any term or provision of this Agreement, the substantially prevailing party in such proceeding will be entitled to recover, in addition to all other relief arising out of this Agreement, such party's

reasonable attorneys' and other experts' (including without limitation accountants) fees and expenses.

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 Main Agreement ;

(c) The processing will comprise: storage and analysis of user login and related data for the purposes of user authentication and user authorization;

(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 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.

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 EU Data Protection Laws 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 EU Data Protection Laws 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

4.1 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 EU Data Protection Laws 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

5.1 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 laws of England.

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 law of England and Wales.

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): ……..

Position: ……..

Address: ……

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

Signature ……

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

Name: ……..

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

Security Measures

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 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).