AUTH0, INC.
DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**DPA**") between Auth0 and Customer contains terms to establish the parties' respective responsibilities under Data Protection Laws (as defined below) with respect to personal data to be processed by Auth0 as a processor pursuant 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 Self Service Terms of Service), that governs Customer's use of Auth0's identity management platform-as-a-service solution (the "**Agreement**"). This DPA is incorporated into and made subject to the Agreement.

By indicating Customer's acceptance of this DPA, or by executing a "**Sales Order**" under the 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 DPA. This DPA is effective between Customer and Auth0 on the date on which Customer indicates its assent to the DPA.

---

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, as applicable: (i) 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) ("**EU GDPR**"), and (ii) the EU GDPR, as incorporated into the law of the United Kingdom under the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), in each case as may be amended or superseded from time to time.

(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**", "**controller**" "**data subject"**, "**supervisory authority**" and "**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 the Customer Data Security Exhibit published at auth0.com/legal. Customer has reviewed Auth0's security measures 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 authorizes 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:

(vii) 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:

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

(b) 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

(c) 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 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 Customer transfers any Personal Data for processing outside of the European Economic Area ("**EEA**") (other than exclusively in an Adequate Country) by Auth0, 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 purposes of the Standard Contractual Clauses, such entities constitute "data exporters".

(b) For the purposes of clause 8.1(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 clause 8.9 of the Standard Contractual Clauses may be exercised as specified in Section 5.2 of this DPA.

(d) Pursuant to clause 9(a) of the Standard Contractual Clauses, Auth0's Affiliates may be retained as sub-processors, and Auth0 and its Affiliates respectively may engage third-party subprocessors 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 9(a) of the Standard Contractual Clauses, Auth0 may engage new subprocessors as described in Sections 4.3 and 4.4 of this DPA. The parties agree that copies of subprocessor agreements that Auth0 must provide to Customer pursuant to clause 9(c) 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 clauses 8.5 and 16(d) 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 (including the Standard Contractual Clauses), 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

Categories of data subjects

Customer may submit Personal Data to the Auth0 Platform the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customers, business partners, and vendors of the data exporter (who are natural persons)
- Employees or contact persons of data exporter customers, business partners, and vendor
- Employees, agents, advisors, contractors, or any user authorized by the data exporter to use the Service (who are natural persons)

Categories of personal data

Customer may submit Personal Data to the Auth0 Platform, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- User profile information as selected by data exporter such as name
- Contact information such as email addresses, phone numbers
- Authentication information based on method selected by data exporter

Sensitive data (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Customer may submit sensitive data to the Auth0 Platform, the extent of which is determined and controlled by the Customer in its sole discretion.

If applicable, Customer agrees that it has reviewed and assessed the restrictions and safeguards applied to the special categories of Personal Data, including the measures described in the Customer Data Security Exhibit published at auth0.com/legal and has determined that such restrictions and safeguards are sufficient.

Nature of the processing

Identity and access management and related services pursuant to the Agreement.

Purpose(s) of the data processing

The objective of Processing of Personal Data by Auth0 is the performance of the Service pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Auth0 may retain Personal Data for the duration of its Agreement with the Customer. Upon termination or expiry of the Agreement, Auth0 shall return or delete the Personal Data in accordance with Clause 3.7 of the DPA.

Approved (sub-) processors, also specify subject matter, nature and duration of the processing

Details of Sub-processors are available at auth0.com/legal.

Exhibit 2
Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

[INTENTIONALLY OMITTED]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection

against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted

by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;[4]

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue

possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

(d) In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(e) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(f) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of France.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name (Customer): ….....

Address ….....

Contact person's name, position and contact details:….....

Activities relevant to the data transferred under these Clauses: Data exporter's use of Auth0 identity and access management cloud service as detailed in one or more Order Form(s) to process Customer Data that is Personal Data in accordance with terms of the Agreement and the Data Processing Addendum.

Data exporter is the legal entity that has executed the Data Processing Addendum based on the Standard Contractual Clauses as a Data Exporter established within the European Economic Area and Switzerland that have purchased the Service on the basis of one or more Order Form(s).

Signature and date: …

Role: controller

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Auth0 Inc

Address: 10800 NE 8th Street, Suite700, Bellevue, WA 98004, U.S.A.

Contact person's name, position and contact details: CFO, legal@auth0.com

Activities relevant to the data transferred under these Clauses: Provision by data importer, Auth0, Inc., of identity and access management cloud services which Processes Personal Data, where such data is Customer Data, upon the instruction of the data exporter in accordance with the terms of the Agreement and the Data Processing Addendum.

Signature and date: …

Role: processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customers, business partners, and vendors of the data exporter (who are natural persons)
- Employees or contact persons of data exporter customers, business partners, and vendor
- Employees, agents, advisors, contractors, or any user authorized by the data exporter to use the Service (who are natural persons)

Categories of personal data transferred

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- User profile information as selected by data exporter such as name
- Contact information such as email addresses, phone numbers
- Authentication information based on method selected by data exporter

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data exporter may submit special categories of data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion.

If applicable, data exporter agrees that it has reviewed and assessed the restrictions and safeguards applied to the special categories of Personal Data, including the measures described in the Customer Data Exhibit published at auth0.com/legal and has determined that such restrictions and safeguards are sufficient.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous for duration of the Agreement

Nature of the processing

Identity and access management and related services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

The objective of Processing of Personal Data by the data importer is the performance of the Service pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data exporter may retain Personal Data in the Service for as long as it deems necessary. Personal Data which is retained outside the Service or within the Service post-termination of the Agreement will be retained in accordance with the terms of the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Details of Sub-processors are available at https://auth0.com/legal.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

Commission nationale de l'informatique et des libertés

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Auth0 shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, including Personal Data, as set forth in the Customer Data Security Exhibit published at auth0.com/legal. Auth0 regularly monitors compliance with these safeguards. Auth0 will not materially decrease the overall security of the Service during a subscription term.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

Auth0 conducts reasonable due diligence and security assessments of Sub-processors engaged by Auth0 in the storing and/or processing of Personal Data, and enters into agreements with Sub-processors that contain provisions similar or more stringent than those provided for in the Customer Data Security Exhibit published at auth0.com/legal. Auth0 will work directly with sub-processors, as necessary, to provide assistance to Customer.

Details of sub-processors are available at auth0.com/legal.