



## **DATA PROCESSING ADDENDUM**

*Based on the General Data Protection Regulation (GDPR) and European Commission Decision 2021/914/EU - Standard Contractual Clauses*

This Data Processing Addendum (“DPA”) forms part of the Master Subscription Agreement (or other such titled written or electronic agreement addressing the same subject matter) between Okta and Customer for the purchase of online identity-as-a-service and access management services (including related Okta offline or mobile components) from Okta (identified collectively either as the “Service” or otherwise in the applicable agreement, and hereinafter defined as the “Service”), wherein such agreement is hereinafter defined as the “Agreement,” and whereby this DPA reflects the parties’ agreement with regard to the Processing of Personal Data. Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Okta processes Personal Data for which such Authorized Affiliates qualify as the Controller or a Processor. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In providing the Service to Customer pursuant to the Agreement, Okta may Process Personal Data on behalf of Customer, and the parties agree to comply with the following provisions with respect to any Personal Data.

This DPA consists of distinct parts: (1) this body and its set of definitions and provisions, and (2) the Standard Contractual Clauses and Annexes I, II, III and IV (if applicable). Please note that the Controller-to-Processor and Processor-to-Processor Standard Contractual Clauses are included by reference and their full text, including Annex III and Annex IV addressing respectively data transfers with Switzerland and the United Kingdom, is available via a link in the definitions of this DPA.

### **INSTRUCTIONS ON HOW TO EXECUTE THIS DPA WITH OKTA**

1. This DPA has been pre-signed on behalf of Okta, Inc., as the data importer.
2. To complete this DPA, Customer must complete the information in the signature box and sign on Page 8.
3. Customer must send the completed and signed DPA to Okta either by (1) email, indicating the Customer’s full entity name (as set out on the applicable Okta Order Form or invoice) in the body of the email, to [DPA@okta.com](mailto:DPA@okta.com); or (2) by completing the DPA digitally, via the link at the following webpage: <https://www.okta.com/trustandcompliance> . Upon receipt of the validly-completed DPA by Okta at either the email address in part (1) or via the web as described in part (2) of the prior sentence, this DPA shall come into effect and legally bind the parties.

### **APPLICATION OF THIS DPA**

If the Customer entity signing this DPA is a party to the Agreement, then this DPA is an addendum to, and forms part of, the Agreement. In such case, the Okta entity (i.e., either Okta, Inc. or a subsidiary of Okta, Inc.) that is party to the Agreement is party to this DPA.



If the Customer entity signing this DPA has executed an Order Form with Okta or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Okta entity that is a party to such Order Form is a party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, then this DPA is not valid and therefore is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

## **DPA DEFINITIONS**

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer entity signing this Agreement, or with Okta, Inc., as the case may be. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“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 and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Service pursuant to the Agreement between Customer and Okta, but has not signed its own Order Form with Okta and is not a "Customer" as defined under the Agreement.

“CCPA” means the California Consumer Privacy Act, California Civil Code sections 1798.100 *et seq.*, as amended by the California Privacy Rights Act of 2020, including any implementing regulations.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Controller to Processor Standard Contractual Clauses” means the agreement executed by and between Customer acting as Controller and Okta acting as Processor and included herein, pursuant to the European Commission’s Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. The Controller to Processor Standard Contractual Clauses are currently available [here](#).

“Customer Data” means all electronic data submitted by or on behalf of Customer, or an Authorized Affiliate, to the Service.

“Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States and its states, applicable to the Processing of Personal Data under the Agreement.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.



“Deidentified Data” means data that cannot reasonably be used to infer information about, or otherwise be linked to, a Data Subject and where such data is Processed only in accordance with the section “Deidentified Data” of this DPA.

“GDPR” means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Okta” means the Okta entity which is a party to this DPA, as specified in the section “Application of this DPA” above, being Okta, Inc., a company incorporated in Delaware and its primary address as 100 First Street, San Francisco California 94105, USA, or an Affiliate of Okta, as applicable.

“Okta Group” means Okta and its Affiliates engaged in the Processing of Personal Data.

“Personal Data” means 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 and Regulations), where for each (i) or (ii), such data is Customer Data.

“Processing” (including its root word, “Process”) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity which Processes Personal Data on behalf of the Controller.

“Processor to Processor Standard Contractual Clauses” means the agreement executed by and between Customer acting as a Processor acting on behalf of a Controller and Okta acting as a Processor on behalf of Customer pursuant to the European Commission’s Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. The Processor to Processor Standard Contractual Clauses are currently available [here](#).

“Standard Contractual Clauses” means either the Controller to Processor Standard Contractual Clauses or the Processor to Processor Standard Contractual Clauses, as currently available [here](#).

“Sub-processor” means any Processor engaged by Okta or a member of the Okta Group.

“Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

“Trust & Compliance Documentation” means the Documentation applicable to the specific Service purchased by Customer, as may be updated periodically, and accessible via Okta’s website at [www.okta.com/agreements](http://www.okta.com/agreements), or as otherwise made reasonably available by Okta.



## DPA TERMS

Okta and the signatory below at the address below (“Customer”) hereby enter into this DPA effective as of the last signature date below. This DPA is incorporated into and forms part of the Agreement.

1. **Provision of the Service.** Okta provides the Service to Customer under the Agreement. In connection with the Service, the parties anticipate that Okta may Process Customer Data that contains Personal Data relating to Data Subjects.

2. **The Parties’ Roles.** The parties agree that with regard to the Processing of Personal Data, Okta acts as Processor on behalf of the Customer, which may act either as a Controller or a Processor, and that Okta or members of the Okta Group will engage Sub-processors pursuant to the requirements of this DPA. For the avoidance of doubt, to the extent Processing of Personal Data is subject to the CCPA, the parties agree that Customer is the “Business” and Okta is the “Service Provider” (as those terms are defined by the CCPA).

3. **Customer Responsibilities.** Customer shall, in its use of the Service, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirements to provide notice to Data Subjects of the use of Okta as Processor. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Service will not violate the rights of any Data Subject that has opted-out from sales, or other disclosures of Personal Data, to the extent applicable under the CCPA or other Data Protection Laws and Regulations.

4. **Processing Purposes.** Okta shall keep Personal Data confidential and shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Service; and (iii) Processing to comply with other documented, reasonable instructions provided by Customer (for example, via email) where such instructions are consistent with the terms of the Agreement. Okta shall not be required to comply with or observe Customer’s instructions if such instructions would violate any Data Protection Laws and Regulations.

5. **Scope of Processing.** The subject-matter of the Processing of Personal Data by Okta is the performance of the Service pursuant to the Agreement and Okta acknowledges that Customer is disclosing or authorizing Okta to collect on Customer’s behalf, or is otherwise making available, Personal Data in connection with this Agreement for the limited purposes set out in the Agreement and this DPA, as specified in Annex I. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex I to the Standard Contractual Clauses attached to this DPA.

6. **Data Subject Requests.** To the extent legally permitted, Okta shall promptly notify Customer if Okta receives a request from a Data Subject to exercise the Data Subject’s right of access, right to rectification,



restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making (“Data Subject Request”). Factoring into account the nature of the Processing, Okta shall assist Customer by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Service, does not have the ability to address a Data Subject Request, Okta shall, upon Customer’s request, provide commercially-reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that Okta is legally authorized to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Okta’s provision of such assistance.

7. **Okta Personnel.** Okta shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training regarding their responsibilities, and have executed written confidentiality agreements. Okta shall take commercially-reasonable steps to ensure the reliability of any Okta personnel engaged in the Processing of Personal Data. Okta shall ensure that Okta’s access to Personal Data is limited to those personnel assisting in the provision of the Service in accordance with the Agreement.

8. **Data Protection Officer.** Members of the Okta Group have appointed a data protection officer. The appointed person may be reached at [privacy@okta.com](mailto:privacy@okta.com).

9. **Sub-processing.**

**9.1 Okta’s Sub-processors.** Customer has instructed or authorized the use of Sub-processors to assist Okta with respect to the performance of Okta's obligations under the Agreement pursuant to a written contract that binds each Sub-processor to comply with applicable Data Protection Laws and Regulations and with terms no less protective of privacy than the terms in this DPA. Okta shall be liable for the acts and omissions of its Sub-processors to the same extent Okta would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

**9.2 List of Okta’s Sub-processors.** A list of Okta’s current Sub-processors, including a description of their processing activities and locations, is made available on Okta’s Agreements webpage (accessible via [www.okta.com/agreements](http://www.okta.com/agreements) under the “Trust & Compliance Documentation” link). Customer acknowledges and agrees that (a) Okta’s Affiliates may be retained as Sub-processors; and (b) Okta and Okta’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Service. On Okta’s Agreements webpage (accessible via [www.okta.com/agreements](http://www.okta.com/agreements) under the “Trust & Compliance Documentation” link), Customer may find a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, to which Customer shall subscribe, and if Customer subscribes, Okta shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to process Personal Data in connection with the provision of the applicable Service.

**9.3 Right to object to a new Sub-processor.** In order to exercise its right to object to Okta’s use of a



new Sub-processor, Customer shall notify Okta promptly in writing within ten (10) business days after receipt of Okta's notice in accordance with the mechanism set out above. In the event Customer objects to a new Sub-processor, and that objection is not unreasonable, Okta will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially-reasonable change to Customer's configuration or use of the Service to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Okta is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those aspects of the Service which cannot be provided by Okta without the use of the objected-to new Sub-processor by providing written notice to Okta. Okta will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Service.

**9.4 Sub-processors and the Standard Contractual Clauses.** Customer acknowledges and agrees that Okta may engage Sub-processors as described in this section for the fulfilment of Okta's obligations under Clause 9(a) of the Standard Contractual Clauses. The parties agree that the copies of the Sub-processor agreements that must be provided by Okta 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 Okta beforehand to protect business secrets or other confidential information; and, that such copies will be provided by Okta, in a manner to be determined in its discretion, only upon request by Customer.

10. **Security Measures.** Okta shall maintain appropriate organizational and technical measures for protection of the security (including protection against unauthorized or unlawful Processing, and against unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Customer Data), confidentiality, and integrity of Customer Data, as set forth in Okta's applicable Trust & Compliance Documentation. Okta regularly monitors compliance with these measures. Okta will not materially decrease the overall security of the Service during a subscription term.

11. **Third-Party Certifications and Audit Results.** Okta has attained the third-party certifications and audit results set forth in the Trust & Compliance Documentation. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Okta shall make available to Customer a copy of Okta's then most recent third-party certifications or audit results, as applicable.

12. **Notifications Regarding Customer Data.** Okta has in place reasonable and appropriate security incident management policies and procedures, as specified in the Trust & Compliance Documentation and shall notify Customer without undue delay after a breach of security that causes the unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Okta or its Sub-processors, of which Okta becomes aware (hereinafter, a "Customer Data Incident"). Okta shall make reasonable efforts to identify the cause of such Customer Data Incident, and take those steps as Okta deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident, to the extent that the remediation is within Okta's reasonable control. The obligations set forth herein shall not apply to incidents that are caused by either Customer or Customer's Users.



13. **Return of Customer Data.** Okta shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and time periods specified in the Trust & Compliance Documentation, unless the retention of the data is requested from Okta according to mandatory statutory laws.

14. **Authorized Affiliates.** The parties agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Okta and each such Authorized Affiliate, subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. An Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Service by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation thereof by an Authorized Affiliate shall be deemed a violation by Customer.

15. **Communications.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Okta under this DPA, and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Authorized Affiliate(s).

16. **Exercise of Rights.** Where an Authorized Affiliate becomes a party to the DPA, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Okta directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall 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 shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together, instead of doing so separately for each Authorized Affiliate.

17. **Liability.** Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Okta, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" 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. Okta's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and shall 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. Each reference to the DPA herein means this DPA including its Appendices.

18. **GDPR and CCPA Compliance.** Okta will Process Personal Data in accordance with the GDPR and CCPA requirements directly applicable to Okta's provision of the Service. For clarity, to the extent applicable to Okta's provision of the Service, Okta shall: (1) Process Personal Data only as set forth in the Agreement and this DPA; and (2) Process Personal Data in compliance with the GDPR and CCPA. Okta agrees to promptly



notify Customer upon becoming aware that Okta can no longer comply with the GDPR or the CCPA, the timing of which notification shall be consistent with applicable legal requirements. Upon Customer's reasonable written notice, Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data to the extent required of Customer under the GDPR and CCPA.

19. **APEC Privacy Recognition for Processors.** Okta has obtained APEC Privacy Recognition for Processors ("PRP") certification and, for the Okta-branded aspects of the Service, shall Process Personal Data submitted to such Service as listed in Okta's PRP certification, which Okta makes available online at <https://www.okta.com/trustandcompliance>. As of the date of this DPA, Okta's PRP certification does not extend to the aspects of the Service branded as 'Customer Identity Cloud' (and which were previously branded as 'Auth0').

20. **EU Cloud Code of Conduct.** Okta has obtained the European Union Cloud Code of Conduct ("EU CCC") privacy certification and, for the Okta-branded aspects of the Service, shall process Personal Data submitted to such Service as listed in Okta's EU CCC certification, which Okta makes available online at <https://www.okta.com/trustandcompliance>. As of the date of this DPA, Okta's EU CCC certification does not extend to aspects of the Service branded as 'Customer Identity Cloud' (and which were previously branded as 'Auth0').

21. **Data Protection Impact Assessment.** Upon Customer's request, Okta shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Okta. Okta shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this section of this DPA, to the extent required under the GDPR.

22. **Standard Contractual Clauses.** The Standard Contractual Clauses apply to:

- (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and,
- (ii) all Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed Order Forms for the Service.

For the purpose of the Standard Contractual Clauses the aforementioned entities shall be deemed "data exporters." If necessary to fulfil its legal obligations, Customer may share a copy of the attached Standard Contractual Clauses with Data Subjects.

23. **Customer's Processing Instructions.** This DPA and the Agreement are Customer's complete and final instructions at the time of signature of the Agreement to Okta for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 8.1 of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data:

- (a) Processing in accordance with the Agreement and applicable Order Form(s);
- (b) Processing initiated by Users in their use of the Service and
- (c) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such





instructions are consistent with the terms of the Agreement.

24. **Audits.** The parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: following Customer’s written request, and subject to the confidentiality obligations set forth in the Agreement, Okta shall make available to Customer information regarding the Okta Group’s compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Trust & Compliance Documentation, to the extent that Okta makes them generally available to its customers. Customer may contact Okta in accordance with the “Notices” section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Okta for any time expended for any such on-site audit at the Okta Group’s then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Okta shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Okta. Customer shall promptly notify Okta and provide information about any actual or suspected non-compliance discovered during an audit. The provision in this section shall by no means derogate from or materially alter the provisions on audits as specified in the Standard Contractual Clauses.

25. **Data Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clauses 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Okta to Customer only upon Customer’s request.

26. **Personal Data Restrictions.** To the extent that Personal Data is subject to the CCPA, Okta shall not (1) “sell” or “share” Personal Data, as those terms are defined under the CCPA, (2) retain, use, disclose, or otherwise Process Personal Data for any purpose other than the business purposes specified in the Agreement or Annex I, or as otherwise permitted by the CCPA, or (3) retain, use, disclose, or otherwise Process Personal Data in any manner outside of the direct business relationship between Customer and Okta, or combine any Personal Data with personal data that Okta receives from or on behalf of any third party or collects from Okta’s own interactions with Data Subjects, except as permitted by the Data Protections Laws and Regulations. For clarity, Customer’s use of the Service to combine Personal Data with personal data that Okta receives from third parties and/or collected from Customer’s or Okta’s own interactions with Data Subjects for the purposes of providing the Service and as noted in the Documentation is deemed a combination authorized by Customer.

27. **Deidentified Data.** To the extent Customer discloses or otherwise makes available Deidentified Data to Okta, or to the extent Okta generates Deidentified Data from Personal Data, Okta shall (1) implement technical safeguards that prohibit re-identification of the User to whom the information may pertain; (2) has implemented business processes that specifically prohibit re-identification of the Deidentified Data and prevent the inadvertent release of De-identified Data; and (3) make no attempt to reidentify the Deidentified Data.

28. **Language.** The governing language of this DPA is English. Any Japanese language version of this DPA is for reference purposes only. If there is any conflict between the English and Japanese version, the English version shall prevail.



29. **Order of Precedence.** This DPA is incorporated into and forms part of the Agreement and the Standard Contractual Clauses are incorporated by reference to this DPA. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

Agreed by Customer:

Agreed by Okta, Inc.:

Signature: \_\_\_\_\_

Signature: *Larissa Schwartz*

By: \_\_\_\_\_

By: Larissa Schwartz

Title: \_\_\_\_\_

Title: Chief Legal Officer

Date: \_\_\_\_\_

Date:



**ANNEXES TO THE STANDARD CONTRACTUAL CLAUSES (IF APPLICABLE)**

***ANNEX I***

**A. LIST OF PARTIES**

**Data exporter(s):**

Name: The entity named as “Customer” in the DPA

Address: The address for Customer associated with its Okta account or as otherwise specified in the DPA or the Agreement.

Contact person’s name, position and contact details: The address for Customer associated with its Okta account or as otherwise specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data, where such data is Customer Data, for the performance of the identity and access management cloud services upon the instruction of the data exporter in accordance with the terms of the Agreement and the DPA.

Signature and date: By executing the DPA, the data exporter will be deemed to have signed this Annex I.

Role: Controller and/or processor

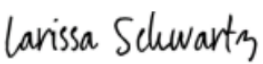
**Data importer(s):**

Name: Okta, Inc.

Address: 100 First Street, San Francisco, California 94105, USA

Contact person’s name, position and contact details: Lisa Turbis, Data Protection Officer, [privacy@okta.com](mailto:privacy@okta.com)

Activities relevant to the data transferred under these Clauses: Processing of Personal Data, where such data is Customer Data, for the performance of the identity and access management cloud services upon the instruction of the data exporter in accordance with the terms of the Agreement and the DPA.

Signature and date:  (March 1, 2023)  
Larissa Schwartz, Chief Legal Officer

Role: Processor on behalf of Customer



## B. DESCRIPTION OF TRANSFER

### *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:

- Identifiers, such as first and last name, ID data, business contact information (company, email, phone, physical business address), and personal contact information (email, cell phone)
- Categories of Personal Data described in subdivision (e) of Section 1798.80 of the CCPA (as defined by this DPA), such as title, position, employer, professional life data, and personal life data (in the form of security questions and answers)
- Internet or other network or device activity details, such as connection data
- Localization data
- Commercial information, such as records of products or services purchased and other transactional data

*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, and which may include Personal Data concerning health information. 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 Trust & Compliance Documentation (as defined by this DPA) and Documentation (as defined in the Agreement), 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)*

Subject to Customer's use of the Service, Personal Data will be transferred on a continuous basis during the term of the Agreement.

*Nature of the processing*

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

*Business 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 and services pursuant to the Agreement and as instructed by data exporter in its use of the Service.

*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 the duration of the Agreement. Personal Data within the Service post-termination of the Agreement will be retained and deleted in accordance with the Documentation.

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

Sub-processors may only Process Personal Data as necessary for the performance of the Service pursuant to the Agreement and for the duration of the Agreement. Sub-processor information are made available on Okta's 'Agreements' webpage (accessible via [www.okta.com/agreements](http://www.okta.com/agreements) under the "Trust & Compliance Documentation" link).

## **C. COMPETENT SUPERVISORY AUTHORITY**

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

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 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 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 shall act as competent supervisory authority.



## *ANNEX II*

### **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

Okta maintains administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, including Personal Data, as set forth in the Trust & Compliance Documentation (accessible via <https://www.okta.com/trustandcompliance/>). Okta regularly monitors compliance with these safeguards. Okta will not materially decrease the overall security of the Service during a subscription term. Okta's Service is designed to permit data exporter to manage Data Subject Requests without assistance from Okta. If data exporter cannot complete its obligations pursuant to a Data Subject Request without assistance from Okta, then, and as set forth in the section "Data Subject Requests" of the DPA, factoring into account the nature of the Processing, Okta shall assist data exporter by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of data exporter's obligation to respond to a Data Subject Request.

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

Okta conducts reasonable due diligence and security assessments of Sub-processors, and enters into agreements with Sub-processors that contain provisions similar to or more stringent than those provided for in the Security & Privacy Documentation within Trust & Compliance Documentation. Okta will work directly with Sub-processors, as necessary, to provide assistance to data exporter.



*ANNEX III*  
**DATA TRANSFERS FROM SWITZERLAND**

In case of any transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland (“Swiss Data Protection Laws”), the following provisions apply:

1. General and specific references in the Standard Contractual Clauses to GDPR, or EU or Member State Law, shall have the same meaning as the equivalent reference in Swiss Data Protection Laws, as applicable.
2. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.
3. Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws.
4. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.





*ANNEX IV*

**DATA TRANSFERS FROM THE UNITED KINGDOM**

In case of any transfers of Personal Data from the United Kingdom, the following provisions apply:

This annex provides the addendum that has been issued by the Information Commissioner for parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Where this annex uses capitalized terms that are defined in the DPA, including the Standard Contractual Clauses, those terms shall have the same meaning as in the Standard Contractual Clauses. Other capitalized terms have the meanings provided by the Addendum B.1.0, issued by the Information Commissioner’s Office and laid before the United Kingdom Parliament in accordance with section 119A of the Data Protection Act 2018 on February 2, 2022.

Part 1: Tables

**Table 1: Parties**

As pursuant to Annex IA – List of the Parties of the DPA

**Table 2: Selected SCCs, Modules and Selected Clauses**

|                         |   |
|-------------------------|---|
| <b>Addendum EU SCCs</b> | The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:<br><br>Date: As pursuant to the effective date of the DPA<br><br>Reference (if any): The relevant modules of the Addendum EU SCCs are available on Okta’s Trust & Compliance Documentation page at <a href="https://www.okta.com/trustandcompliance/">https://www.okta.com/trustandcompliance/</a><br><br>Other identifier (if any): not applicable |
|-------------------------|---|

**Table 3: Appendix Information**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:



Annex 1A: List of Parties: Page 11 of the DPA

Annex 1B: Description of Transfer: Pages 12 to 14 of the DPA

Annex II: Technical and organisational measures, including technical and organisational measures to ensure the security of the data: Page 15 of the DPA

Annex III: The list of Sub-processors is available on Okta's Trust & Compliance Documentation page at <https://www.okta.com/trustandcompliance/>

**Table 4: Terminating this Addendum when the Approved Addendum Changes**

|   |   |
|---|---|
| <b>Terminating this Addendum when the Approved Addendum changes</b> | Which Parties may terminate this Addendum as set out in section 19 of the Approved Addendum:<br><input checked="" type="checkbox"/> Importer<br><input type="checkbox"/> Exporter<br><input type="checkbox"/> neither Party |
|---|---|

Part 2: Mandatory Clauses

|                          |  |
|--------------------------|--|
| <b>Mandatory Clauses</b> | Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before the United Kingdom Parliament in accordance with section 119A of the Data Protection Act 2018 on February 2, 2022, as it is revised under section 18 of those Mandatory Clauses. |
|--------------------------|--|

# okta