OKTA, INC.
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Master Subscription Agreement (or other written or electronic agreement governing Customer's use of the Service) (the "**Agreement**") between Okta and Customer. 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 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 Affiliates, if and to the extent Okta processes Personal Data for which such Affiliates qualify as the Controller or a Processor.

This DPA consists of distinct parts: (1) the main body of the DPA, and (2) the Standard Contractual Clauses and Annexes I, II, III, and IV (if applicable). Please note that the Standard Contractual Clauses are included by reference, and their full text, including Annex III and Annex IV addressing respectively data transfers from Switzerland and the United Kingdom, is available on the Trust & Compliance Documentation.

INSTRUCTIONS ON HOW TO EXECUTE THIS DPA WITH OKTA

1. This DPA has been pre-signed on behalf of Okta, Inc.

2. Customer must complete the information in the signature box and sign on the signature page.

3. Customer must send the completed and signed DPA to Okta either (1) via 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 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.

4. If Customer makes any deletions or revisions to this DPA, such deletions or revisions are hereby rejected and invalid unless agreed in writing by Okta. Customer's signatory represents and warrants that they have the authority to bind Customer to this DPA.

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.

If the Customer entity signing this DPA has executed an Order Form with Okta 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 an entity should request that the Customer entity who is a party to the Agreement executes this DPA.

DPA DEFINITIONS

"**Affiliate**" has the meaning set forth in the Agreement. If undefined, "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.

"**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, as superseded, amended, and replaced.

"**Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.

"**Customer Data**" means all electronic data submitted by or on behalf of Customer, or an Affiliate, to the Service.

"**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Economic Area (EEA), and their member states, Switzerland, the United Kingdom, and the United States and its states, Canada and its provinces, applicable to the Processing of Personal Data under the Agreement, as superseded, amended, or replaced.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**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), as superseded, amended, or replaced.

"**Okta**" means Okta Inc.

"**Personal Data**" means any information relating to an identified or identifiable natural person that is included within Customer Data. For clarity, Personal Data includes equivalent definitions under Data Protection Laws and Regulations, such as "personally identifiable information" and "personal information" to the extent such information is part of 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 automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

"**Restricted Transfe**r" means (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the Swiss FADP applies, a transfer of Personal Data from Switzerland to any country which is not recognized to provide adequate protection by the Swiss Federal Data Protection and Information Commission; and (iii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Security Breach**" means 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.

"**Standard Contractual Clauses**" means the Standard Contractual Clauses 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 (Module 2) and the Processor to Processor Standard Contractual Clauses (Module 3) are currently available here.

"**Sub-processor**" means any Processor engaged by Okta to Process Personal Data on Okta's behalf in order to provide the Service.

"**Supervisory Authority**" means (i) "Supervisory Authority" as defined in the GDPR; or (ii) "Commissioner" in the context of the UK GDPR and the Federal Data Protection and Information Commissioner, where applicable.

"**Swiss FADP**" means the Swiss Federal Act on Data Protection 2020, as superseded, amended, or replaced.

"**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 https://www.okta.com/trustandcompliance/, or as otherwise made reasonably available by Okta.

"**UK GDPR**" means the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

"**U.S. Privacy Laws**" means specifically the Data Protection Laws and Regulations in the United States and its states, including the CCPA, applicable to the Processing of Personal Data under the Agreement.

okta

DPA TERMS

Okta and Customer hereby enter into this DPA effective as of the last signature date below:

1. **Scope of Processing.** Okta provides the Service to Customer under the Agreement. In connection with the Service, the parties anticipate that Okta may Process Personal Data. 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.

2. **The Parties' Roles.** The parties agree that with regard to the Processing of Personal Data:

   (i) Okta acts as a Processor on behalf of Customer, and Customer acts as a Controller, unless Customer is the processor of the Personal Data. In that case, Okta is a Sub-processor to Customer;

   (ii) 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. Customer shall have the 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 under Data Protection Laws and Regulations.

4. **Purpose Limitation.** 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 and applicable Data Protection Laws and Regulations.

   4.1 Customer's Processing Instructions. This DPA and any applicable Agreement constitute Customer's complete and final instructions at the time of execution of this DPA for the purposes described above. Any additional or alternate instructions outside the scope of the Agreement or this DPA for the Processing of Personal Data must be agreed upon by both Parties and documented.

   4.2 Lawfulness of Instructions. Customer's instructions to Okta for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Okta shall not be required to comply with or observe Customer's instructions if such instructions would violate any Data Protection Laws and Regulations. If Okta becomes aware or reasonably believes that Customer's instructions do not comply with Data Protection Laws and Regulations, Okta will notify Customer. Okta will inform Customer upon becoming aware that Okta can no longer comply with its obligations under this DPA and the GDPR.

5. **Data Subject Request(s).** Okta may provide Customer with self-service features to assist Customer in responding to requests from Data Subjects to exercise their data subject rights under Data Protection Laws and Regulations ("Data Subject Request"). To the extent the Services do not provide such features, or Customer is unable to address a Data Subject Request without assistance, Okta, factoring into account the nature of Processing, shall, to the extent possible, assist Customer by appropriate technical and organizational measures. If a Data Subject Request is made directly to Okta regarding the Processing of Personal Data, and to the extent Customer is identified or can easily be identified by Okta, Okta will redirect the Data Subject to submit their request to Customer. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from the provision of additional assistance requested by Customer to address a Data Subject Request.

6. **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 privacy and security training regarding their responsibilities, and have executed written confidentiality agreements.

7. **Sub-processing.**

7.1 Okta's Sub-processors. Customer acknowledges and agrees to Okta's use of Sub-processors. Where the Standard Contractual Clauses apply, the parties acknowledge that Customer provides a general consent to onward sub-processing by Okta. Okta must: (i) enter into 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, and (ii) remain 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.

7.2 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 our Okta Sub-processor Information Page, within our Trust & Compliance Documentation (https://support.okta.com/help/s/article/okta-sub-processor-information?language=en_US). 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.

7.3 New Sub-processors. Customer may subscribe to receive notifications of new Sub-processor(s) for each applicable Okta Service, by sending an email to subprocessors@okta.com with the following information: (i) Customer Name, (ii) Customer Address, (iii) Executed copy of the Customer-Okta DPA, and (iv) Customer e-mail address. Okta shall use this mechanism to provide notification of any new Sub-processor before it authorizes any such new Sub-processor(s) to process Personal Data in connection with the provision of the applicable Service.

7.4 Right to Object. Customer may object to Okta's use of a new Sub-processor by notifying Okta in writing at privacy@okta.com. Customer shall notify Okta promptly in writing within thirty (30) 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 such change available within a reasonable time period, which shall not exceed thirty (30) business 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.

7.5 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.

8. **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.

9. **Third-Party Certifications and Audit Results.** Okta has attained certain third-party certifications and audit results that are made available to Customer for self-service viewing at security.okta.com.

10. **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:

(i) following Customer's written request, and subject to the confidentiality obligations set forth in the Agreement, Okta shall make available to Customer information regarding Okta's compliance with the obligations set forth in this DPA, to the extent that Okta makes it generally available to its customers.

(ii) 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 Okta'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 in writing 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.

(iii) 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.

11. **Notifications Regarding Security Breaches.** 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 confirming a Security Breach. Okta shall make reasonable efforts to identify the cause of such Security Breach, and take those steps as Okta deems necessary and reasonable in order to remediate the cause of such a Security Breach, 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.

12. **Deletion and Return of Personal Data.** Upon termination of the Agreement, Okta shall make available to Customer its Personal Data and delete Personal Data in accordance with the procedures and time periods specified in the Trust & Compliance Documentation, unless the retention of the Personal Data is permitted by Okta under applicable Data Protection Laws and Regulations. 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 written request.

13. **Data Protection Impact Assessment and Prior Consultations.** Upon Customer's written request, Okta shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Data Protection Laws and Regulations 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 Data Protection Laws and Regulations.

14. **Standard Contractual Clauses.** Where the transfer of Personal Data involves a Restricted Transfer, the Standard Contractual Clauses (or the UK Addendum, where applicable) apply to the legal entity that has executed the Standard Contractual Clauses, and its Affiliates, as data exporters and Okta as a data importer. By entering into this DPA, the Parties are deemed to be signing the applicable Standard Contractual Clauses (including the UK Addendum) and its applicable Appendices and Annexes, which are incorporated herein by this reference.

15. **U.S. Privacy Laws.** As required by applicable U.S. Privacy Laws, Okta agrees to:

(i) not (1) "sell" or "share" Personal Data, as those terms are defined under U.S. Privacy Laws; (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 U.S. Privacy Laws; (3) retain, use, disclose, or otherwise Process Personal Data in any manner outside of the direct business relationship between Customer and Okta; or (4) 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 U.S. Privacy Laws.

(ii) Upon Customer's reasonable written notice, Customer may take reasonable and appropriate steps to ensure that Okta uses Personal Data in a manner consistent with Customer's obligations under U.S. Privacy Laws.

(iii) In the event Customer determines that Okta has used Personal Data in a manner inconsistent with U.S. Privacy Laws, Customer may, upon Customer's reasonable written notice, stop and remediate such unauthorized use of Personal Data.

(iv) promptly notify Customer upon becoming aware that Okta can no longer comply with U.S. Privacy Laws, the timing of which notification shall be consistent with applicable legal requirements.

(v) comply with its obligations under U.S. Privacy Laws.

16. **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 Affiliate(s). All access to and use of the Service by Affiliate(s) must comply with the terms and conditions of the Agreement and any violation thereof by an Affiliate shall be deemed a violation by Customer.

17. **Communications and Exercise of Rights.** 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 Affiliate(s). The parties agree that (i) solely Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Affiliate, and (ii) 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 Affiliates together, instead of doing so separately for each Affiliate.

18. **Liability.** Each party's and all of its Affiliates' liability for all claims, taken together in the aggregate, arising out of or related to the Agreement and this DPA, and all DPAs between Affiliates and Okta, is subject to the "Limitation of Liability" section of the Agreement. Okta's and its Affiliates' total liability shall not be understood to apply individually and severally to Customer and/or to any Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA, including its Appendices.

19. **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 or French version, the English version shall prevail.

20. **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 obligations 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: _____

okta

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 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

Activities relevant to the data transferred under these Clauses: Processing of Personal 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.

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 vendors
- 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, social logins, business contact information (company, email, phone, physical business address), and personal contact information (email, cell phone, address)
- Professional details, 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

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 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

To provide 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 the duration of the Agreement. Personal Data within the Service post-termination of the Agreement will be retained and deleted in accordance with the Trust & Compliance 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 provision of the Service pursuant to the Agreement and for the duration of the Agreement. Sub-processor information is made available on the "Trust & Compliance Documentation".

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. Okta regularly monitors compliance with these safeguards. Okta will not materially decrease the overall security of the Service during a subscription term.

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 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 Standard Contractual Clauses apply with the following modifications:

1. General and specific references in the Standard Contractual Clauses to GDPR, EU, EEA or Member State Law, shall have the same meaning as the equivalent reference in Swiss Data Protection Laws, as applicable.

2. 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.

3. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

okta

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

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: As pursuant to the effective date of the DPA Reference (if any): The relevant modules of the Addendum EU SCCs are available on Okta's Trust & Compliance Documentation page at https://www.okta.com/trustandcompliance/ 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 7 of the DPA
Annex 1B: Description of Transfer: Pages 7 of the DPA

Annex II: Technical and organisational measures, including technical and organisational measures to ensure the security of the data: Page 10 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

Terminating this Addendum when the Approved Addendum changes	Which Parties may terminate this Addendum as set out in section 19 of the Approved Addendum: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Mandatory Clauses	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.