Data Processing Addendum (formerly SaaS Addendum)

This Data Processing Addendum ("**DPA**") is incorporated into the software agreement and/or services agreement ("**Agreement**") between Provider and Customer for the purchase of certain SaaS Software licenses and/or Maintenance Services and/or professional services (for purposes of this DPA hereinafter referred to as "**Services**") and forms part of a written (including in electronic form) contract between Provider and Customer. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions.

Capitalized terms not defined in context or in the Agreement shall have the meanings assigned to them below:

a) "***Controller***" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

b) "***Data Protection Law***" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("**CCPA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended, or replaced from time to time.

c) "***Data Subject***" means the identified or identifiable natural person to whom Customer Personal Data relates.

d) "***Personal Data***" means information about an identified or identifiable natural person, or that otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

e) "***Personal Data Breach***" means an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third party access to Customer Personal Data being Processed by Provider, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

f) "***Processing***" refers to any operation that is performed on 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.

g) "***Processor***" means a natural or legal person, public authority, agency, or other body that Processes Personal Data on behalf of the Controller.

h) "***Standard Contractual Clauses***" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

i) "***Sub-processor***" means Provider's Affiliates and third parties engaged by Provider (or by Provider's Affiliates) for the provision of any or all part(s) of the Services and who processes Customer Personal Data in accordance with this DPA.

2. Processing of Customer Personal Data.

Provider may Process Customer Personal Data under the Agreement as a Processor acting on behalf of Customer as Controller (or as subprocessor, as applicable, on behalf of Customer as Processor). Provider undertakes to Process Personal Data for the sole purpose of performing Provider's obligations to Customer under and in accordance with: (i) this DPA and the Agreement, and (ii) Customer's written instructions, or (iii) to comply with Provider's obligations under applicable laws, subject to any notice requirements under Data Protection Laws. Details of the subject matter of the Processing, its duration, nature and purpose, and the type of Customer Personal Data, and Data Subjects, are as specified in the Agreement, or, if not specified, shall be as set out in Annex 1 of the Appendix to this DPA. Customer and Provider agree to comply with their respective obligations under Data Protection Laws applicable to the Personal Data that is Processed in connection with the Services. Customer has sole responsibility for complying with Data Protection Laws concerning the Processing of Customer Personal Data prior to disclosing, transferring, or otherwise making available, any Personal Data to Provider. Provider shall immediately inform Customer if, in its opinion, Customer's instructions would be in breach of Data Protection Laws.

3. Security of Processing.

a) **General Security Policies**. Provider will implement and maintain technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data, and that protect against Personal Data Breaches, in accordance with Provider's security measures referenced in the Agreement and as further described at https://www.oneidentity.com/legal/security.aspx (collectively "***Security Site***") including the following:

- Information Security Policy,
- Statement of Technical and Organizational Measures,
- Data Breach Response Policy, and
- Privacy Policy.

Provider may modify its Security Site so long as it does not materially decrease the overall level of protection provided.

b) **Confidentiality**. Provider will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement. Provider will ensure that Provider personnel who Process Customer Personal Data have entered into written confidentiality agreements with Provider. Provider shall ensure that such confidentiality obligations survive the termination of employment for any such personnel. Provider will regularly train Provider personnel that have access to Customer Personal Data, in data security and data privacy requirements and principles.

4. Data Subject Requests.

Upon Customer's request, Provider will use commercially reasonable measures to assist Customer in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Services). If Provider receives a Data Subject request in relation to Personal Data being processed hereunder, Provider will advise the Data Subject (where the Data Subject has provided information to identify the Customer) to redirect its request to Customer.

5. Audit Rights.

a) **Provider Records Generally.** Provider will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's written request, make available to Customer any records reasonably necessary to demonstrate compliance with Provider's obligations under this DPA and applicable Data Protection Laws.

b) **Third-Party Compliance Program.** Provider will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request (subject to the confidentiality obligations set out in the Agreement). Customer may share a copy of Audit Reports with relevant government authorities as required.

c) **Customer Audit.** Customer may, at Customer's expense, conduct an audit pursuant to a mutually agreed-upon plan that is consistent with the audit parameters below (an "**Audit**"). Customer may exercise its Audit rights (1) to the extent Provider's provision of an Audit Report does not provide sufficient information for Customer to verify either Provider's compliance with this DPA or compliance with Data Protection Laws; or (2) as necessary for Customer to respond to a government authority audit, or (3) in connection with a Personal Data Breach.

Each Audit must 1) be conducted by an independent third party that will have entered into a confidentiality agreement with Provider, (2) be limited in scope to matters reasonably required for Customer to assess Provider's compliance with this DPA and the parties' compliance with Data Protection Laws, (3) occur at a mutually agreed date and time and only during Provider's regular business hours, (4) occur no more than once annually (unless required under Data Protection Laws or in connection with a Personal Data Breach), (5) cover only facilities controlled by Provider, (6) restrict findings to Customer Personal Data only, and (7) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

6. Sub-processors and International Transfers.

a) **Use of Sub-processors.** Customer generally authorizes Provider to engage Sub-processors in connection with the provisioning of the Services. Provider shall execute the appropriate written agreements with Sub-processors in accordance with the provisions of this DPA and the instructions herein between Customer and Provider. Provider is responsible for any breaches of this DPA to the extent caused by Sub-processors engaged by Provider.

b) **Subprocessor List.** Provider maintains lists of Sub-processors per Software Product, including their functions and locations, available to Customer through registration at https://support.oneidentity.com/subprocessor. At least thirty (30) days before authorizing any new Sub-processor to access Personal Data, Provider will update the list of Sub-processors and notify Customer through email upon registration.

c) **Objection to New Sub-processors.** If Customer does not approve of a new Sub-processor, then Customer may terminate any subscription for the applicable SaaS Software by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval.

d) **International Transfers.** For the transfer of European and / or UK Personal Data to a Sub-processor located in a third country that does not provide adequate protection for Personal Data, Provider and the applicable Subprocessor have entered into the EU SCCs in order to provide appropriate safeguards for the transfer of such Personal Data in accordance with the European and UK Data Protection Laws.

7. Personal Data Breach Notification.

In addition to the obligations set forth in the Security Site, Provider will promptly notify Customer after becoming aware of a Personal Data Breach and provide reasonable information to assist Customer to meet Customer's obligation to report a Personal Data Breach as required under Data Protection Laws. Provider may provide such information in phases as it becomes available. Provider agrees to make good faith efforts to identify the cause of a Personal Data Breach and take steps as Provider deems necessary and reasonable to remediate the cause of the Personal Data Breach.

8. Deletion of Customer Personal Data.

Unless Customer notifies Provider at least thirty (30) days before the completion of the Services, following termination or expiration of the Agreement, Provider will delete all Customer Personal Data from Provider's systems. Provider will perform deletion in accordance with industry-standard secure deletion practices. Notwithstanding the foregoing, Provider may retain Customer Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Provider will (1) maintain the confidentiality of, and otherwise comply with, the applicable provisions of this DPA with respect to retained Customer Personal Data and (2) not further Process retained Customer Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

9. Data Protection Impact Assessment.

Provider shall provide Customer with reasonable cooperation and assistance, as needed, to fulfil Customer's obligations under Data Protection Laws to carry out a data protection impact assessment or similar risk assessment related to Customer's use of the Services.

APPENDIX

This Appendix forms part of the DPA.

ANNEX I - Subject Matter and Details of Processing

A. LIST OF PARTIES

The Agreement between Customer as the controller and Provider as the Processor contains a description of all the required information, such as:

- name, address, contact person's name,
- position and contact details,
- activities relevant to the data transferred under these Clauses, and
- signature and date.

B. DESCRIPTION OF PROCESSING

1. Categories of Data Subjects whose personal data is processed

Unless provided otherwise by Customer, processed Personal Data relates to the following categories of Data Subjects:

- employees, contractors, business partners of Customer.

2. Categories of Personal Data processed

Customer determines the categories of data per its use of the Services. The Personal Data Processed typically concern the following categories of data:

- employment details (which may include company name and address, job title, grade, demographic and location data) relating to employees of Customer or other third parties whose personal information is provided by or on behalf of Customer;
- system information related to Customer systems, or systems provided to Provider by Customer and related to the Services purchased under the Agreement and required for the provisioning of Services (which may include user ID and password, computer and domain name, the IP address, GUID number or location of the computer or other device being used).

Customer Personal Data processed may concern past, present, and prospective, business partners or other individuals related to such business partners.

3. Sensitive data processed (if applicable)

Special categories of Personal Data (sensitive data) must not be provided by Customer unless identified on a case-by-case basis, and then only to the extent that the parties agree that such special categories of data are to be covered by the provision of the Services.

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

Continuously for the duration of the use of the Services.

5. Nature of the Processing

a) Maintenance Services: Provider or its Subprocessors provide Maintenance Services when a Customer submits a support ticket because the Software is not available or not working as expected. Provider answers phone calls and perform basic troubleshooting, and handle support tickets in a tracking system.
b) Professional services: Provider or its Subprocessors provide Services subject to the Services Order.
c) SaaS Software: provision of the SaaS Software purchased by Customer.

6. Purpose(s) of the data transfer and further processing

Customer Personal Data Processed by Provider will be subject to the following basic Processing activities:

a) Use of Personal Data to provide the Provider Services and where applicable, to provide access to and benefits of the SaaS Software pursuant to the Agreement and to provide Maintenance Services at Customer's request and in accordance with Customer's specific requirements, as appropriate, all in accordance with the instructions described below;
b) Storage of Personal Data;
c) Computer processing of Personal Data for data transmission;
d) Continuous improvement of service features and functionalities provided as part of the Provider Services including automation, transaction processing, and machine learning;
e) Execution of Customer's instructions in accordance with the Agreement.

The following additional Processing activities apply to any Personal Data stored in the SaaS Software:

a) Storage of Personal Data in data centers (multi-tenant architecture);
b) Back up and restoration of Customer Personal Data stored in the SaaS Software;
c) Computer processing of Personal Data including data transmission, data retrieval, and data access;
d) Communication to Customer's users;
e) Release, development, and upload of any fixes or upgrades to the SaaS Software;

f) Network access to permit Personal Data transfer;
g) Monitoring, troubleshooting, and administering the underlying SaaS Software infrastructure and database;
h) Security monitoring, network based intrusion detection, and penetration testing; and
i) As necessary to respond to and address requests and demands of Data Subjects as appropriate and in accordance with the instructions described below.

Provider may use anonymized data (which is not Customer Personal Data but may be derived from Customer Personal Data) for purposes related to product improvement and development of new Provider Products and Services.

Further details of what the SaaS Software does, how it handles Personal Data, and the data storage location are indicated in the applicable Product Documentation and Security Guide.

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.
The Personal Data shall be Processed during Customer's use of the Services pursuant to the Agreement and subject to Section 8 of this DPA.

8. For transfers to Sub-processors, also specify subject matter, nature and duration of the Processing
In respect of the EU SCCs, transfers to Sub-processors shall be on the same basis as set out in this DPA.

9. Instructions, Customer and Provider Commitments
Provider will follow written and documented instructions received from Customer with respect to Customer Personal Data unless in Provider's opinion such instructions (1) are legally prohibited or likely to result in a violation of applicable Data Protection Law, (2) require material changes to Provider's Services, and/or (3) are inconsistent with the terms of the Agreement or Provider's Documentation relating to the Services sold under the Agreement. In any such case, Provider shall immediately inform Customer of its inability to follow such instructions. Any description of Processing in the Agreement, this DPA, and any related Documentation of Provider shall be considered as instructions by Customer.

ANNEX II - Statement of Technical and Organizational Measures

Provider will use the appropriate technical and organizational measures that are set out on the Security Site (as defined in Section 3(a) of the DPA) in Provider's Processing of Customer Personal Data. Provider may modify the measures taken in protecting Customer Personal Data as long as it does not materially decrease the overall level of data protection provided for herein.