Omada Data Processing Addendum

Last Updated: February 17th, 2025

This Data Processing Addendum ("**DPA**") forms part of the Customer Agreement and applicable Orders between Omada and Customer (the "**Agreement**") and shall be effective on the effective date of the Agreement.

1. DEFINITIONS

The terms listed in this Section 1 shall have meanings ascribed for the purposes of this DPA. Capitalized terms used in this DPA that are not defined in this Section 1 (Definitions) shall have the meaning ascribed to them elsewhere in this DPA and/or the Agreement or in applicable Data Protection Laws unless otherwise specified.

"**Approved Purpose**" means the Processing required to fulfill the purpose of the Agreement and provide the applicable Omada Offerings set forth on an Order, as further described in Schedule A

"**Customer**" means the party identified in the applicable Order in effect between Customer and Omada that governs Customer's use of, and Omada's provision to Customer of, specific Omada Solution Offering.

"**Customer Personal Data**" means any Personal Data that is submitted, disclosed, provided or otherwise made available to Omada (either directly or indirectly) by or on behalf of Customer for Processing, under or in connection with the Omada Offerings.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Information under the Agreement, provided that such laws are no more prescriptive than the European General Data Protection Regulation or any other law specifically referenced herein, including, but not limited to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA**"), and other applicable U.S. state privacy laws.

"**Personal Data**" means: any information (i) relating to an identified or identifiable natural person; or (ii) defined as "personally identifiable information", "personal information", "personal data" or similar terms, as such terms are defined under Data Protection Laws.

"**Process**", "**Processes**", "**Processing**", and "**Processed**" means any operation or set of operations performed upon Personal Data, whether or not by automatic means.

"**Security Incident**" or **"Data breach"** means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data on systems managed by or otherwise controlled by Omada.

"**Source(s)**" means a Customer-managed or subscribed to target system for reading data from, and if supported by the specific system, writing changes to, user accounts.

"**Sub-processor**" or "**Subprocessor**" means any entity engaged by Omada or its Affiliates to assist in fulfilling its obligations with respect to providing Services to Customer. Sub-processors may include third parties or Omada's Affiliates. Sub-processors may also include subcontractors that are specified in an applicable Order which form part of the Agreement.

2. SCOPE AND JURISDICTION-SPECIFIC ADDENDA

2.1. **Applicability**. This DPA applies to the Processing of Personal Data that is subject to Data Protection Laws.

2.2. **Jurisdictional Addenda**. Attached to this DPA is the United States Privacy Law Addendum as Schedule D and the European Addendum as Schedule E, each of which provide terms specific to the Processing of Customer Personal Information arising out of specific legal requirements from those jurisdictions. In the event that Customer Personal Data is Processed from one or more of these jurisdictions, and the applicable requirements are not already covered in this DPA, then the terms in the respective Addendum attached hereto shall apply solely with respect to Customer Personal Data subject to the applicable legal requirements of such jurisdiction(s). In the event of a conflict between the Agreement or this DPA and an Addendum, the Addendum applicable to Customer Personal Data from the relevant jurisdiction shall control with respect to Customer Personal Data from that relevant jurisdiction, and solely with regard to the portion of the provision in conflict. In the event Customer believes Customer Personal Data is processed within the scope of additional jurisdictions, which require additional Addenda to be attached to this DPA, Customer has the sole responsibility for notifying Omada and working with Omada to effectuate such Addenda. Such additional Addenda shall apply subject to the requirements of this Section 2.

3. ROLES

3.1. **Roles**. The parties acknowledge and agree that Customer is a Controller of Customer Personal Data and Omada is a Processor of Customer Personal Data for the purposes of applicable Data Protection Laws. The specific rights, duties, and responsibilities of the Controller and Processor, or equivalent roles, shall be governed and interpreted in accordance with applicable Data Protection Laws.

3.2. **Controller**. The Controller is responsible for ensuring that: (i) Personal Data is Processed in compliance with applicable

Data Protection Laws and this DPA; and (ii) there is a legal basis for the Processing performed by the Processor. The Customer has the right to change the Approved Purpose and means of the Processing of Personal Data by written notice to the Processor.

3.3. **Processor**. The Process is responsible for Processing the Personal Data for the Approved Purpose and in accordance with applicable Data Protection Laws, this DPA and the Agreement.

3.4. **Customer Processing of Personal Data.** Customer: (i) agrees that it will comply with its obligations under Data Protection Laws in respect of its Processing of Personal Data and any Processing instructions it issues to Omada; and (ii) represents and warrants that it has provided all fair processing notices and obtained all consents and rights necessary under Data Protection Laws for Omada to Process Personal Data and provide the Omada Solution Offering pursuant to the Agreement and this DPA.

3.5. **Customer Instructions.** Omada will Process Customer Personal Data only: (i) for the Approved Purpose; and (ii) in accordance with Customer's documented lawful instructions and applicable Data Protection Laws. Omada will not Process Customer Personal Data provided by or collected on behalf of Customer for any purpose except as necessary to maintain or provide the Omada Offerings specified in the Agreement and this DPA, or as necessary to comply with the law or binding order of a governmental body to which Omada is subject. In this case, Omada shall inform Customer of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Except as the parties may agree to otherwise in writing, the parties agree that this DPA, including all applicable Addenda, and the Agreement set out the Customer's complete instructions to Omada in relation to the Processing of Customer Personal Data by Omada.

3.6. **Environments**. The Processing may only take place in technological environments controlled by the Controller, the Processor and subcontractors in the jurisdictions set out in Schedule C.

3.7. **Details of Processing**. Details of the Processing of Customer Personal Data are set out in Schedule A.

4. SUB-PROCESSING

4.1. **Authorization of Sub-processors**. The Processor may engage subcontractors for the fulfilment of this DPA. Customer understands and hereby authorizes Omada to engage Sub-processors and Affiliates to Process Customer Personal Data Customer's behalf as listed on Schedule C.

4.2. **Changes**. If required under applicable Data Protection Laws, Omada shall notify Customer, in writing, of any intended additional or replacement Sub-processor who will Process Customer Personal Data at least thirty (30) days prior to when the Sub-processor begins Processing Customer Personal Data (such period, the "**Review Period**"). As required or permitted under applicable Data Protection Laws, Customer may object to any additional or replacement Sub-processor at any time during the Review Period as follows: (i) any objections raised by Customer during the Review Period may only be based on reasonable grounds and only with respect to data protection concerns; and (ii) Customer may object to Omada's additional or replacement Sub-processor under Section 4.2 of this DPA by providing notice of Customer's objection, in writing, and in the manner provided in the Agreement. Omada will have a reasonable time to notify Customer, in writing, that the proposed addition or replacement shall not apply to any of the Omada Solution Offering provided by Omada to the Customer or allow the Customer to terminate for convenience the affected Order used by Customer, and in the manner provided in the Agreement. Customer will continue to pay all fees for the affected Omada Solution Offering until the termination takes effect, and if required by law, Customer will receive on a pro-rated basis, net of applicable Partner margins, any unused and prepaid fees covering the remainder of the term of the terminated Order following the effective date of termination. The parties agree that any non-response by the Customer during the Review Period will be taken as the Customer's approval of additional or replacement Sub-processors, where Customer continues to use the Omada Offerings after the Review Period has lapsed. THIS SECTION 4.2 AND, IF APPLICABLE, CLAUSE 9(A) OF THE SCCS, STATE THE ENTIRE LIABILITY OF OMADA AND THE SOLE REMEDY FOR CUSTOMER IN CONNECTION WITH ANY OBJECTION BY CUSTOMER TO AN INTENDED ADDITIONAL OR REPLACEMENT SUB-PROCESSOR WHO WILL PROCESS CUSTOMER PERSONAL INFORMATION.

4.3. **Sub-processor Obligations**. Omada will: (i) not engage a Sub-processor unless Omada enters into a written agreement with the Sub-processor which contain obligations that are at least as restrictive as those set out in this DPA, including observing all of the applicable requirements as required in applicable Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any failure by a Sub-processor engaged by Omada to fulfil its data protection obligations under the applicable Data Protection Laws.

5. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

5.1. **Security Measures**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Omada shall implement and maintain appropriate technical and organizational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and Confidential of the Customer Personal Data, in accordance with Omada's security standards described in Schedule B, as applicable to the Omada Offerings ("**TOMs**"). Customer is responsible for reviewing the TOMs and making an independent determination as to whether such TOMs meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the TOMs are subject to technical progress and development and that Omada may update or modify the TOMs from time-to-time provided that such updates and modifications do not result in a material degradation of the overall security of the Omada Offerings.

5.2 **Customer Responsibilities**. Customer agrees that, without prejudice to Omada's obligations under Section 5.1 (Security Measures) and Section 8.2 (Security Incident Response), Customer is responsible for its use of the Omada Solution Offering, including: (i) making appropriate use of the Omada Solution Offering to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; (ii) securing its account authentication credentials; (iii) protecting the security of Customer Personal Data when in transit to and from the Omada Offerings; (iv) taking appropriate steps to securely encrypt and/or

backup any Customer Personal Data uploaded to the Omada Solution Offering; and (v) properly configuring the Omada Solution Offering and using available features and functionalities to maintain appropriate security in light of the nature of the Customer Personal Data Processed as a result of Customer's use of the Omada Solution Offering. Omada has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Omada's and its Sub-processors' (where applicable) systems (for example, offline or on-premises storage).

6. DATA SUBJECT AND LAW ENFORCEMENT REQUESTS

6.1. **Data Subject Request Assistance**. Omada shall, at the request of the Customer, and taking into account the nature of the Processing, provide reasonable cooperation to assist Customer to respond to any requests from data subjects in relation to their data subject rights as required under applicable Data Protection Laws ("**Data Subject Request(s)**") relating to the Processing of Customer Personal Data under the Agreement, provided that (i) Customer is itself unable to respond without Omada's assistance and (ii) Omada is able to do so in accordance with all applicable laws, rules, and regulations. Omada shall apply appropriate technical and organizational measures needed to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance under this Section 6.1. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Omada.

6.2. **Requests Made to Omada**. Omada shall promptly notify Customer of any request it has received from the data subject. Omada shall not respond to the request itself, unless authorized to do so by Customer. Customer shall bear the responsibility for responding to all such requests. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Omada if needed for Customer to fulfill a Data Subject Request, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each data subject.

6.3. **Law Enforcement Request**. If a law enforcement agency sends Omada a demand for Customer Personal Data, such as a subpoena or court order, Omada will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Omada may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Data to a law enforcement agency, then Omada will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Omada is legally permitted to do so.

6.4. **Notice of Request**. If Omada is legally required to respond to a request enumerated in Sections 6.2 and 6.3, Omada will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

7. COMPLIANCE, REPORTS, AND AUDITS

7.1. **Compliance with Legal Obligations**. Upon Customer's written request at reasonable intervals, Omada shall (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Omada's compliance with its obligations, as required of Omada under applicable Data Protection Laws; and (ii) allow and cooperate with reasonable inspections or audits, as required or permitted under applicable Data Protection Laws.

7.2. **Security Reports**. Upon request, Omada shall provide to Customer (on a Confidential basis) a summary copy of any third-party audit report(s) or certifications applicable to the Omada Offerings ("**Report**"), so that Customer can verify Omada's compliance with this DPA, the audit standards against which it has been assessed, and the standards specified in the TOMs, as described in Schedule B.

7.3. **Security and Audit Questionnaires**. If Customer reasonably believes that the Report provided is insufficient to demonstrate compliance with this DPA, Omada shall also provide written responses (on a Confidential basis and at Customer's request and expense) to reasonable requests for information made by Customer related to its Processing of Customer Personal Data, including responses to information security and audit questionnaires that are reasonably necessary to demonstrate Omada's compliance with this DPA, provided that Customer shall not be permitted to exercise this right more than once every 12 months.

7.4. **Audits**. If Customer reasonably believes that the information provided pursuant to Sections 7.1, 7.2 and/or 7.3 is insufficient to demonstrate compliance with this DPA, Omada will allow an audit by Customer (that is not a competitor of Omada or auditors appointed by Customer and reasonably acceptable to Omada) in relation to Omada's Processing of Customer Personal Data. Any such audit will be at Customer's expense, with reasonable advance notice, which shall be no less than thirty (30) days, conducted during normal business hours, carried out no more than once every 12 months and subject to Omada's reasonable security and Confidential requirements, provided that the exercise of rights under this Section would not infringe Data Protection Laws.

7.5. **Data Protection Impact Assessments**. Taking into account the nature of the Processing and information available to Omada, Omada shall (at Customer's request and expense) provide reasonably requested information regarding the Omada Offerings to enable the Customer to carry out data protection impact assessments and prior consultations with the competent supervisory authority as required under applicable Data Protection Laws.

8. CONFIDENTIAL AND SECURITY INCIDENT RESPONSE

8.1. **Confidential of Processing**. Omada shall maintain the Confidential of Personal Data provided by Customer and shall ensure that any person who is authorized by Omada to Process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of Confidential (whether a contractual or statutory duty).

8.2. **Security Incident Response**. Omada shall: (i) taking into account the nature of Omada's Processing of Customer Personal Data and the information available to Omada, notify Customer of a Security Incident that it becomes aware of, without undue delay; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer, including providing information sufficient to enable Customer to meet its obligations under applicable Data Protection Laws to notify the competent supervisory authority and/or the data subjects affected by the Security Incident; and (iii) promptly

take reasonable steps to contain, investigate, and mitigate any Security Incident.

8.3. **Notification**. Customer acknowledges that Omada will not assess the contents of Customer Personal Data in order to identify information subject to any specific legal requirements. Customer is solely responsible to comply with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incidents as required by Data Protection Laws. Unless otherwise required under Data Protection Laws, the parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected data subjects and/or notices to the relevant supervisory authorities.

8.4. **Data Retention**. Upon Customer's written request, Omada shall delete or return all Personal Data provided by Customer, unless retention of such Personal Data is required or authorized by law or the DPA and/or the Agreement.

9. GENERAL TERMS

9.1. **Changes**. When Customer renews or purchases Omada Solution Offering, the then-current DPA terms will apply during the term of the Order for such Omada Solution Offering. In the event of changes to applicable Data Protection Laws, including, but not limited to, the amendment, revision, or introduction of new laws, regulations, or other legally binding requirements to which either party is subject, Omada may revise the terms of this DPA and issue any appropriate or necessary updates in good faith, including the addition, amendment, or replacement of any Addenda. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Data. This DPA will terminate automatically with the termination or expiry of the Agreement, subject to additional provisions in any Addenda attached hereto.

9.2. **Exclusions and Limitations**. Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement. Without limiting either of the parties' obligations under the Agreement, Customer agrees that any regulatory penalties incurred by Omada that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Omada's liability under the Agreement as if it were liability to the Customer under the Agreement.

9.3. **Applicable Contracting Entity**. Any claims against Omada or its Affiliates under this DPA shall only be brought by the Customer entity that is a party to the Agreement against the Omada entity that is a party to the Agreement. In no event shall this DPA or any party to this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

9.4. **Governing Law**. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

SCHEDULE A

INFORMATION ABOUT THE PROCESSING

1. The Approved Purpose is:

Providing software and services in the field of identity governance

2. The nature and type of Processing:

Providing software and services in the field of identity governance by the Data Processor to the Data Controller

3. The Processing includes the following types of Personal Data:

Choose the applicable types of Personal Data that are being Processed:

☒ Name
☐ Address
☐ Telephone number
☐ National identification number
☒ Job title
☒ Employee ID
☐ Language preference
☐ Other:_____

4. The Processing includes the following categories of Data Subjects:

Choose the applicable types of Data Subjects that are being Processed:

☒ Employees
☒ External Support
☒ Consultants
☒ Representatives
☐ Other:_____

Special categories (Art. 9 GDPR) will not be provided by the Data Controller.

5. The Processing has the following duration:

The Data Processor can Process the Personal Data for the duration of the Agreement.

SCHEDULE B

OMADA TOMS

Omada has implemented and shall maintain a commercially reasonable security program in accordance with industry best practices, which shall include technical and organizational measures to ensure an appropriate level of security for Customer Personal Data taking into account the risks presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to Customer Personal Data, and the nature of the Customer Personal Data to be protected having regard to the state of the art and the cost of implementation. Omada's security program shall include the following measures:

DATA PRIVACY CONTROLS

I. Omada Security Certifications

Omada Identity Cloud services meet the specific requirements of data protection, including Article 28 of the General Data Protection Regulation which are listed as SOC 2, Type 2 and ISO 27001 compliant an others.

At a minimum, Omada has implemented for the Omada Identity Cloud the technical and organizational measures and maintains security practices within the production environments as follows:

II. Confidentiality Measures

Physical Access Management

a) Employee physical access that is no longer required in the event of personnel termination or role change is promptly revoked. If applicable, temporary badges are returned before exiting the facility.

b) Initial permission definitions and changes to permissions, associated with physical access roles are approved by appropriate Omada personnel.

Physical Access Reviews

Omada performs physical access account reviews every quarter; corrective action is taken where applicable.

Physical Security

a) Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points and/or manned reception desks.

b) All facilities require badge access and have 24x7 security guards. Some facilities use additional measures to prevent unauthorized individuals from tailgating authorized individuals into the facility.

c) Intrusion detection and video surveillance are installed at all facilities. Omada may review video logs when issues or concerns arise to determine access.

d) Omada power and telecommunication lines are protected from interference, interception and damage.

e) Granting physical access to an Omada data center requires management approval and documented specification of:

(1) account type: (visitor, vendor, or regular)

(2) intended business purpose

(3) visitor identification method, if applicable

(4) temporary badge issued, if applicable

(5) access start date and end date

(6) access duration

f) Visitors to a facility are required to be always escorted and are not allowed in caged areas.

g) Visitor Access Logs are retained for up to 12 months following Omada's documentation retention policy.

Logical access

a) Logical access provisioning to information systems requires approval from appropriate personnel.

b) Logical access that is no longer required in the event of termination is documented, communicated to management, and revoked.

c) Omada performs account and access reviews quarterly, and corrective action is taken where applicable.

Authentication

a) Omada creates unique identifiers for user accounts and prevents the reuse of identifiers. Account Login parameters follow these rules:

(1) Accounts are not shared;

(2) Inactive sessions are password protected after 15 minutes; and

(3) All systems classified as confidential and restricted require multifactor authentication. Multifactor authentication must be used for access to environments that host production systems or systems and applications containing restricted or confidential data.

b) Omada users are enrolled with the Omada Identity Cloud platform. Omada Identity Cloud platform is a platform that uses multifactor authentication plus device and security posture during authentication. For more information on the Omada Identity Cloud platform, see the Omada white paper available here: https://omadaidentity.com/resources/product-brief/

(1) Omada Identity Cloud access proxy is encrypted with Transport Layer Security (TLS).

(2) Users enrolled in the Omada Identity Cloud platform are only required to change their passwords upon compromise indicator.

(3) Access to the system needs to be requested every day, as it is revoked every day, at midnight. Authentication is based on 2FA.

c) In case of circumstances where an Omada user is not enrolled with the Omada Identity Cloud platform, user and device authentication to information systems is protected by passwords that meet Omada's password complexity requirements.

Strong password configurations adhere to the following rules:

a) Omada enforces the use of complex Windows passwords.
b) All Omada business critical systems are protected by the two-factor authentication.
c) Unless Omada Identity Cloud is cloud-enabled, remote connections to the corporate network are accessed via VPN through managed gateways.

Role-Based Access Control

a) Initial permission definitions and changes to permissions associated with logical access roles are approved by the appropriate personnel.

b) Access that allows modification to source code is restricted to authorized personnel.

c) Role-based and context-based access to data are modelled on the concept of least privilege.

Network Operations

a) Omada maintains a dedicated Support Center which is staffed 24/7 with at least 2 dedicated personnel.

b) Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established following identified security requirements and business justifications.

c) Omada uses Web Application Firewalls, network zones isolation and strict protocol controls as layers of security. Antivirus is running on all employee desktops and laptops and all email traffic is scanned for malware. Additionally, real-time antivirus scanning is enabled.

d) Production environments are logically segregated from non-production environments.

Key Management

Omada uses encrypted, centrally managed cryptographic key stores. Access to the cryptographic key stores is limited to authorized personnel, it is logged and reviewed as defined by the process.

Preservation and Review of Security Logs

a) Omada keeps logs used in connection with its security procedures for the protection of Personal Data related to the applicable product operations in a secure location. Omada retains logs within the Security Event Monitoring and logs aggregation service, for a minimum period of one year.

b) Security event logs are reviewed per the event context and severity, some of which require daily review.

III. Employee Management

Background Checks and Non - Disclosure Agreements

a) For business-critical functions, Omada obtains pre - hire background check reports for employment purposes. The specific nature and scope of the report that Omada typically seeks may include (as permitted or required by applicable law):

(1) Educational background;

(2) Work history;

(3) Court records (including criminal conviction records); and

(4) References obtained from professional and personal associates.

b) Omada hires employees based on a documented job description.

c) Employees are required to sign a Non-Disclosure Agreement upon employment. Omada employees including contractors are required to sign an agreement that they will protect confidential information.

Training and Awareness

a) Omada personnel (including contract workers) complete security awareness training, which includes annual updates about relevant policies, standards, and new or modified attack vectors and how to report security events to the appropriate response team. Records of annual training

completion are documented and retained for tracking purposes. Any Omada vendors with network access are required to complete their own equivalent security awareness training.

b) Annually, Omada full-time and temporary employees and interns complete a code of business conduct training. Anyone who is found to violate the Code of Business Conduct or other Omada policies may be subject to disciplinary action including termination of employment or contract.

IV. Information Systems and Technology Management

Production Configuration Management

a) Omada ensures security hardening and baseline configuration standards have been established according to industry standards defined by the Microsoft Security Baseline (Security baselines guide - Windows Security | Microsoft Learn) and are reviewed and updated periodically.

b) Omada uses mechanisms to detect deviations from baseline configurations in production environments.

c) Installation of software or programs in the production environment requires approval by the appropriate personnel.

Change Management

a) Change scope, change type, and roles and responsibilities are pre-established and documented in a change control workflow. Notification and approval requirements are also pre-established based on the risk associated with change scope and type. Change management uses an automated ticketing system.

b) Based on risk, before introducing changes into the production environment, approval from appropriate personnel is required based on the following:

(1) Change description is documented;

(2) Impact of change;

(3) Test results are documented; and

(4) Back-out procedures are defined.

c) Changes to the production environment are implemented by authorized personnel only.

Data Transfer

a) Omada deploys dedicated network connections from its corporate offices to Omada data center facilities to enable secure management of the servers.

b) All management communications to the servers occur over encrypted tunnels and sessions. Some examples are Secure Shell (SSH), Transport Layer Security (TLS); Internet Protocol Security (IPSec) and Virtual Private Network (VPN) channels. Remote access for VPN always requires multifactor authentication.

c) Administrative data is encrypted in transit across the internet via TLS 1.2 or greater over HTTPS between the Customer and the user interface.

d) All customer data is encrypted with Transparent Data Encryption (TDE) using AES256.

e) All environments and components are pseudonymized.

f) Right to be forgotten. Omada Identity Cloud setup with its true data isolation allows deletion of all data from the customer environment when requested.

g) Account closure and deletion of data. Upon the end of the subscription (whether through expiry or termination), the Customer no longer has rights to access or use the Services, including the associated Omada software. Within 30 days after the effective date of termination or expiration of this Agreement, Omada will make the Customer Data available to the Customer for export or download as provided in the Documentation. After the 30 days, Omada has no obligation to maintain or provide any Customer Data and, as provided in the Documentation, must delete, or destroy all copies of Customer Data in its systems or otherwise in its possession or control, unless legally prohibited. Notwithstanding the foregoing, in the event of termination of this Agreement and/or the applicable Order, Omada may make the Customer Data available to the Customer for a longer period by mutual agreement and at fees negotiated by the parties. The Customer may, in addition, request Omada to assist in the extraction of Customer Data. Such assistance requires a separate statement of work (SoW) and must be compensated on a time and material basis applying Omada's then-current price rates for such services.

Security Governance

a) Corporate Documents. Omada's key business functions and information security capabilities are supported by documented procedures that are communicated to authorized personnel.

b) Information Security Management. Omada has an established governance framework that supports relevant aspects of information security with policies and standards.

c) Security Leadership & Roles. Roles and responsibilities for the governance of Information Security within Omada are formally documented and communicated by Management.

Cloud Services Systems Monitoring

a) Critical Information System Logs.

(1) Omada utilizes a centralized Security Event Monitoring solution to aggregate and correlate log events.

(2) To protect against unauthorized access and modification, Omada captures network logs, operating system logs, application logs and security events.

(3) Application user activity is logged by the application.

b) Security Monitoring and Evaluation

(1) Omada defines security monitoring alert criteria, how alert criteria will be flagged and identifies authorized personnel for flagged system alerts.

(2) Omada defines availability monitoring alert criteria, how alert criteria will be flagged and identifies authorized personnel for flagged system alerts. Customers can monitor a product's availability at: https://status.omada.cloud

c) System Design Documentation.

(1) Documentation of system boundaries and key aspects of their functionality are published to authorized Omada personnel.

(2) Omada publishes public-facing whitepapers that describe the purpose, design, and boundaries of the system and system components which are available here: Cloud Identity Management Solution | Omada Enterprise SaaS (omadaidentity.com)

Service & Product Lifecycle

a) Source code is checked for vulnerabilities before being released into production. For high-risk services and products, manual security testing, and, where appropriate, manual and automated code review, is performed for significant changes to ensure detection and prevention of common security issues.

b) All software releases are subject to the Service Life Cycle, which requires acceptance via Concept Accept and Project Plan Commit phases before implementation.

Vulnerability Management

a) Information Systems and Technology.

1. For customer‐facing products as defined in Omada's Current List of Certifications, Standards, and Regulations listed at The Trusted Partner for Modern IGA | Omada Trust Center (omadaidentity.com), at least annually, Omada engages with specialized third parties to perform application penetration testing, assign risk ratings to discovered vulnerabilities, and track vulnerabilities through resolution. At least annually, Omada will perform network penetration testing for all critical services defined in the above list. Network testing may be performed by Omada's internal security teams.

2. The objective of penetration testing is to find security vulnerabilities following industry standards and best practices (such as those listed in the Open Web Application Security Project current ten most common web application security risks).

3. Upon receipt of the deliverable provided by a third party, Omada documents these vulnerabilities, evaluate them following its internal processes as well as recommendations by the third party, and then creates a mitigation strategy or remediation plan.

4. A remediation report which provides an overview of the testing methodologies, findings and remediations can be requested from an Omada sales representative.

b) If applicable, Omada has managed enterprise antivirus deployments and ensures the following:

1. Signature definitions are updated daily;

2. Full scans are performed weekly and real-time scans are enabled; and

3. Alerts are reviewed and resolved by the appropriate personnel.

c) Vulnerability Scans. External and internal vulnerability scans are performed on a continuous basis.

d) Vulnerability Reviews. Omada reviews reasonable customer vulnerability-related inquiries for advisement only.

e) Patch Management. Omada installs security-relevant patches, including software or firmware updates following Omada's patch management standard.

V. Measures for prompt recoverability & access to Data

Incident Response

Omada has implemented a comprehensive incident response program that includes at least the measures below and as described at the The Trusted Partner for Modern IGA | Omada Trust Center (omadaidentity.com)

a). Omada defines the types of incidents that need to be managed, tracked, and reported. Such management includes the following:

1. Procedures for the identification and management of incidents.

2. Procedures for the resolution of confirmed incidents.

3. Key incident response systems.

4. Incident coordination and communication strategy.

5. Contact method for internal parties to report potential incidents.

6. Support team contact information.

7. Notification to relevant Omada management in the event of a security breach.

8. Provisions for updating and communicating the plan.

9. Provisions for the training of the support team.

10. Preservation of incident information; and,

11. Management review and approval (either annually or when major changes to internal organization occur).

b) Omada responds to confirmed incidents and resolution is tracked with appropriate management channels. If applicable, Omada coordinates the incident response with business contingency activities.

c) Omada provides a contact method for external parties to report incidents here: https://omadaidentity.com/company/contact-us/

Disaster Recovery and Business Continuity Plans

a) Omada maintains disaster recovery and business continuity plans and processes to allow for the continuation of the services and to provide an effective and accurate recovery. Such plans are tested on an annual basis.

b) Within the Disaster Recovery process, the following objectives have been defined:

1. Recovery Point Objective (RPO) – a time measurement from the loss event to the most recent preceding backup – 15 minutes

2. Recovery Time Objective (RTO) – the duration of time between loss and recovery. The objective also accounts for the steps internal technical departments have to take to restore the application and it's data – 240 minutes.

c) Within the Disaster Recovery topic we may differentiate two layers – the data layer and infrastructure layer. The data layer consists of databases that are stored within the Azure environment and can be recovered directly by the customer via the Customer Portal

d) All used resource types are operated redundantly in the data centers of an Azure Region (Azure zone-redundant). Back-ups are mirrored in a second Azure region. If the customer subscribes to Omada's geo-redundancy package, the application's data are mirrored in a third Azure region as well.

e) The different data backup types and the time said backups are being stored for the production environment are as follows:

Backup Type	Time
Pont-in-time-recovery (PiTR)	0 Days – 7 Days
Full Weekly	1 Week – 52 Weeks (total of 52 backups)
Full Monthly	1 Month – 12 Months (total 12 backups)
Full Yearly	1 Year – 5 Years (total 5 backups)

VI. Processes for regular testing, assessing, and evaluating the effectiveness of security measures

Risk Management

a) Omada management performs an annual risk assessment in alignment with the ISO/IEC 27001:2013 - Information Security Management Systems and ISO 31000:2009 - Risk Management Principles and Guidelines. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.

b) Management assesses the design and operating effectiveness of internal controls against the established controls framework. Corrective actions related to identified deficiencies are tracked to resolution.

c) Omada establishes internal audit requirements and executes audits on information systems and processes at planned intervals.

d) Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.

Third-Party Management

a) Periodically, management reviews controls within third-party assurance reports to ensure that they meet organizational requirements. If control gaps are identified in the assurance reports, management addresses the impact that disclosed gaps have on the organization.

b) Any Third-Party contract changes applied to Omada services, are a subject of the Risk Assessment process.

Technical Progress

Omada´s Technical and Organizational Measures are subject to technical progress and further development. Accordingly, Omada reserves the right to modify the Technical and Organizational Measures provided that the functionality and security of the Omada Identity Cloud are not degraded.

Notification to Omada

a) To notify Omada of a security issue, please send an email to: security@omadaidentity.com

b) For the data privacy matters, please send an email to: dataprotection@omadadentity.com

SCHEDULE C

SUB-PROCESSORS

Omada use third-party Sub-processors to provide infrastructure for the Omada Identity Cloud, and to aid in e.g., providing customer support and other ancillary services used by the organization to e.g., interact with partners, prospects, and customers. These Sub-Processors have access to personal information (PII) only to assist Omada in the processing of data which has been authorized. They are also authorized according to Sec. 9 to have Personal Data transferred to them and processed in the named rider "Process locations". The Customer can use the system in a way to avoid such transfer as described below in the rider "Personal Data" below.

Omada does not sell or otherwise share customers personal information with any other entities.

Prior to engaging any third party, Omada performs due diligence to evaluate privacy, security, and Confidential practices, and executes an agreement implementing its applicable obligations.

Omada Identity Cloud

The below Sub-processors are used in the delivery of the Omada Identity Cloud to our customers:

Sub-processor	Purpose	Scope	Personal Data	Processing location	Transfer mechanism
Microsoft Corporation (if EU is selected: Microsoft Ireland Operations, Ltd.)	Public cloud network, storage, and compute (Microsoft Azure)	Omada Identity Cloud environments in the EU delivery zone	All data of the IGA platform only if the Customer requests this in writing or activates EU as an Azure region in the cloud environment	European Union	
Microsoft Corporation (if US is selected)	Public cloud network, storage, and compute (Microsoft Azure)	Omada Identity Cloud environments in the North American delivery zone	All data of the IGA platform only if the Customer requests this in writing or activates US as an Azure region in the cloud environment	United States	EU-U.S. Data Privacy Framework
Twilio SendGrid	E-mail delivery	Omada Identity Cloud environments configured for Omada to deliver system generated mails (an option in the self-service management portal)	Name and email address of selected Customer admin accounts if provided by customer. The customer may use non-personal email addresses to avoid processing of personal data	European Union and United States	EU-U.S. Data Privacy Framework

Data importers in the USA listed above are certified under the EU-U.S. Data Privacy Framework.

General and ancillary services

Omada uses the below Sub-processors for other areas of our business:

Sub-processor	Purpose	Scope	Personal Data	Processing location	Transfer mechanism
Microsoft Ireland Operations, Ltd.	E-mail & collaboration platform (Microsoft 365)	Communication and collaboration between Omada employees and partners/customers	All PII the customer decides to share by email or a collaboration tool provided by Microsoft	European Union	
Microsoft Ireland Operations, Ltd.	Project and task management tool (Azure DevOps) used in project delivery	Project delivery based on the IdentityPROCESS+ methodology lead by the Omada Customer Success organization	All data of the IGA platform as setup by customer	European Union	
Freshworks, Inc.	ITSM system used for incident and problem management	Communication and collaboration platform used by the Omada Helpdesk when aiding partners and customers	Name and email address of selected Customer admin accounts if provided by customer. The customer may use non-personal email-addresses to avoid processing of personal data	United States	EU-U.S. Data Privacy Framework

Fuse Universal Ltd	Learning platform used for product documentation and collaboration	Access to product documentation, knowledgebase, and collaboration platform for partners and customers	Name and email address of Customer admin accounts if provided by customer. The customer may use non-personal email-addresses to avoid processing of personal data	United Kingdom	Adequacy decision
Absorb Technology Ltd.	Learning platform used for product documentation and collaboration	Access to Omada Academy Training, product documentation, knowledgebase, and collaboration platform for partners and customers	Name, company name, email address of learner/user	European Union	
Aha!	Product planning and roadmap tool	Platform for partners and customer to request and vote for product capabilities	Name and email address of Customer admin accounts if provided by customer. The customer may use non-personal email-addresses to avoid processing of personal data	United States	EU-U.S. Data Privacy Framework
Salesforce	CRM tool used to store partner and customer information	Prospects, customer and partner information	Name and email address and job title of the customer key contacts	European Union	
Precisely	Contract management system	Active and historic contracts	Name and email and IP address of the signees and key contacts of the contracts between customer and Omada	European Union	
Ciklum ApS	First line technical super user/expert incident and problem management	When partner and customers are requesting support from Omada Helpdesk	Name and email address of registered customer admin accounts if provided by customer. The customer may use non-personal email-addresses and sanitize any logfiles to avoid processing of personal data	Ukraine	Standard Contractual Clauses
DocuSign	Contract and legal document sign-off system	Active and historic contracts	Name and email and IP address of the signees and key contacts of the contracts between customer and Omada	European Union	

Subsidiaries

The below list of fully owned entities may be involved in the delivery of Omada Solution Offering, including without limitation, Omada On Prem:

Sub-processor	Purpose	Scope	Personal Data	Processing location	Transfer mechanism
Omada Solutions Inc.	Engineering, consulting and support services	(If not the OCE*) Consulting services, and support for partners and customers	All data of the IGA platform as setup by customer	United States	Intra Company DPA with Standard Contractual Clauses
Omada Solutions Ltd.	Engineering, consulting and support services	(If not the OCE*) Consulting services, and support for partners and customers	All data of the IGA platform as setup by customer	United Kingdom	Adequacy decision
Omada A/S	Engineering, consulting and support services	(If not the OCE*) Consulting services, and support for partners and customers	All data of the IGA platform as setup by customer	Denmark	
Omada GmbH	Engineering, consulting and support services	Software development, consulting services, and support for partners and customers	All data of the IGA platform as setup by customer	Germany	

Omada Poland Sp. z o.o.	Engineering, consulting and support services	Software development, consulting services, and support for partners and customers	All data of the IGA platform as setup by customer	Poland	
Omada Identity Spain, SL	Engineering, consulting and support services	Software development, consulting services, and support for partners and customers	All data of the IGA platform as setup by customer	Spain	
Omada Sweden AB	Engineering, consulting and support services	Software development, consulting services, and support for partners and customers	All data of the IGA platform as setup by customer	Sweden	

*OCE means the applicable Omada entity entering into the Agreement as set forth therein.

SCHEDULE D

UNITED STATES PRIVACY LAW ADDENDUM

This United States Privacy Law Addendum ("**US Addendum**") supplements the DPA and includes additional information required by the US Data Protection Laws that are not otherwise addressed in the DPA. All words or phrases used herein not defined in this US Addendum will have the meaning assigned to them in the DPA and/or the Agreement.

1. CALIFORNIA

1.1 Definitions. For purposes of this Section 1, the terms "**Business**," "**Business Purpose**," "**Commercial Purpose**," "**Consumer**," "**Personal Data**," "**Processing**," "**Sell**," "**Service Provider**," "**Share**," and "**Verifiable Consumer Request**" shall have the meanings set forth in the CCPA. All references to "**Personal Data**," "**Controller**," "**Processor**," and "**Data Subject**" in the DPA shall be deemed to be references to "**Personal Data**," "**Business**," "**Service Provider**," and "**Consumer**" as defined in the CCPA.

1.2 Obligations.

(a) The parties acknowledge and agree that Customer is a Business and Omada is a Service Provider for the purposes of the CCPA (to the extent it applies) and Omada is receiving Personal Data from Customer to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.

(b) Customer will disclose Personal Data to Omada only for the limited and specified purposes described in the DPA.

(c) Omada will not Sell or Share Personal Data provided by Customer under the Agreement.

(d) Omada will not retain, use, or disclose Customer Personal Data provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the CCPA.

(e) Omada will not retain, use, or disclose Personal Data provided by Customer pursuant to the Agreement outside of the direct business relationship between Omada and Customer, except where and to the extent permitted by the CCPA.

(f) Omada will notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA.

(g) Except and to the extent permitted by the CCPA, Omada will not combine Personal Data received from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

(h) Omada will comply with all obligations applicable to Service Providers under the CCPA, including by providing Personal Data provided by Customer under the Agreement the same level of privacy protection required by CCPA.

(i) Omada shall only engage a new Sub-processor to assist Omada in providing the Services to Customer under the Agreement, in accordance with Section 4 (Sub-Processing) of the DPA, including, without limitation, by: (i) notifying Customer of such engagement at least ten (10) days before enabling a new Sub-processor; and (ii) entering into a written contract with the Sub-processor requiring Sub-processor to observe all of the applicable requirements set forth in the CCPA.

1.3 Consumer Rights. Omada shall assist Customer in responding to Verifiable Consumer Requests to exercise the Consumer's rights under the CCPA as set forth in Section 6 (Data Subject and Law Enforcement Requests) of the DPA.

1.4 Audit and Remediation Rights

(a) To the extent required by the CCPA, Omada shall allow Customer to conduct inspections or audits in accordance with Section 7 (Compliance, Reports, and Audits) of the DPA.

(b) If Customer determines that Omada is Processing Personal Data in an unauthorized manner, Customer may, taking into account the nature of Omada's Processing and the nature of the Personal Data Processed by Omada on behalf of Customer, take commercially reasonable and appropriate steps to stop and remediate such unauthorized Processing.

SCHEDULE E

EUROPEAN ADDENDUM

This European Addendum ("**European Addendum**") supplements the DPA and includes additional information required by European Data Protection Law (as defined below). All words or phrases used herein not defined in this European Addendum will have the meaning assigned to them in the DPA and/or the Agreement.

1. Scope

This European Addendum shall apply in the event that: (i) Omada Processes Customer Personal Data on the behalf of Customer as a Processor in the course of providing Services pursuant to the Agreement; and (ii) Customer is subject to European Data Protection Law and acts as a Controller thereunder, or Omada is subject to European Data Protection Law and acts as a Processor thereunder.

2. Definitions

2.1 "**Data Privacy Framework**" means, collectively, the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce; as may be amended, superseded or replaced.

2.2 "**EEA**" means, for the purposes of this DPA, the European Economic Area.

2.3 "**European Data Protection Law**" means: (i) the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**") as implemented by countries within the EEA; (ii) the European Union e-Privacy Directive 2002/58/EC as implemented by countries within the EEA; (iii) to the extent that Omada Processes any Personal Data subject to the data protection laws in the United Kingdom of Great Britain and Northern Ireland (collectively, the "**UK**"), all laws relating to data protection, the processing of personal information, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR (as defined in section 3 of the Data Protection Act 2018) and the Data Protection Act 2018 (collectively "**UK Privacy Law**"); (iv) to the extent that Omada Processes any Personal Data subject to the data protection laws in Switzerland, the Swiss Federal Act on Data Protection ("**FADP**"); and/or (v) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i), (ii), (iii), and (iv) above.

2.4 "**SCCs**" means, collectively, (i) where Personal Data of data subjects in the EEA is involved, the Standard Contractual Clauses as approved by the European Commission in the form set out in Commission Implementing Decision (EU)2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to GDPR ("**EU SCCs**"), and (ii) where Personal Data of data subjects in the UK is involved, the EU SCCs as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A(1) Data Protection Act 2018 ("**UK SCCs**"), in each case, as completed as described in Section 4 below.

2.5 All terms used herein not defined in the DPA will have the meaning assigned to them in the applicable European Data Protection Law. All references to Data Protection Law or laws in the DPA shall be read in the context of EU or Member State law for the purpose of this Addendum.

3. Cooperation

3.1 Customer acknowledges that Omada may be required under European Data Protection Law to: (i) collect and maintain records of certain information, including the name and contact details of each Processor and/or Controller on behalf of which Omada is acting and, where applicable, of such Processor's or Controller's local representative and data protection officer; and (ii) make such information available to the supervisory authorities. Accordingly, if European Data Protection Law applies to the Processing of Customer Personal Data, Customer will, where requested, provide such information to Omada, and will ensure that all information provided is kept accurate and up-to-date.

4. Standard Contractual Clauses

4.1 To the extent that Omada Processes any Customer Personal Data from the EEA, the UK, or Switzerland, and transfers such Customer Personal Data outside of the EEA, the UK, or Switzerland to the United States of America ("**US Transfers**"), the SCCs shall apply in accordance with Section 4.2 of this European Addendum.

4.2 To the extent that Omada Processes any Customer Personal Data from the EEA, the UK, or Switzerland, and transfers such Customer Personal Data outside of the EEA, the UK, or Switzerland to countries not deemed by the European Commission, the UK Information Commissioner's Office, or Switzerland to provide an adequate level of data protection ("**Restricted Transfers**"), the SCCs will apply to any Restricted Transfers from Customer and Customer Affiliates (each as "data exporter") to Omada (as "data importer") as follows:

(a) **EU Personal Data**. In respect of Personal Data that is protected by the EU GDPR, the EU SCCs will apply for any Restricted Transfers, are incorporated by reference, and are completed as follows:

(i) Module 2 applies;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and will be completed and subject to Section 4 (Sub- processors) of the DPA;

(iv) in Clause 11, the optional redress language will not apply;

(v) in Clause 17, Option 2 will apply, and the EU SCCs will be governed by the law specified in the Agreement, provided that law is an EU Member State law recognizing third party beneficiary rights, otherwise, the laws of the applicable supervisory authority determined under Clause 13 of the EU SCCs shall govern;

(vi) in Clause 18(b), disputes shall be resolved before the courts specified in the Agreement, provided these courts are located in an EU Member State, otherwise those courts shall be the courts of the EU Member State of the applicable supervisory authority determined under Clause 13 of the EU SCCs; and

(vii) in all cases the parties satisfy any signature requirement in "Annex 1: List of Parties" to the EU SCCs by the execution or acceptance of Customer and Omada to the binding Agreement effective between the parties.

(b) **UK Personal Data**. In respect of Personal Data that is protected by the UK Privacy Law, the UK SCCs will apply for any Restricted Transfers, are incorporated by reference, and are completed as follows:

(i) Table 1 of the UK SCCs is completed with the relevant information in Section 4.2(d) of the European Addendum;

(ii) Table 2 of the UK SCCs is completed with the selected modules and clauses from the EU SCCs as identified in Section 4.2(a) of the European Addendum;

(iii) Table 3 of the UK SCCs is completed with the relevant information in Sections 4.2(d) and 4.2(e) of the European Addendum;

(iv) both the importer and the exporter may terminate the UK SCCs in Table 4 of the UK SCCs in accordance with the terms of the UK SCCs; and

(v) in all cases the parties satisfy any signature requirement in UK SCCs by the execution or acceptance of Customer and Omada to the binding Agreement effective between the parties.

(c) **Swiss Personal Data**. In respect of Personal Data that is protected by the FADP, the EU SCCs as completed in Section 4.2(a) will apply for any Restricted Transfers, are incorporated by reference, and are amended as follows:

(i) references to (articles in) the EU General Data Protection Regulation 2016/679 shall be deemed to refer to (respective articles in) the FADP;

(ii) reference to the competent supervisory authority in Annex I. C. under Clause 13 of the SCCs shall be deemed to refer to the Federal Data Protection and Information Commissioner ("**FDPIC**");

(iii) references to Member State(s)/EU Member State(s) shall be deemed to include Switzerland;

(iv) reference to the European Union in Annex I (A) shall be deemed to include Switzerland;

(v) where the Clauses use terms that are defined in the GDPR, those terms shall be deemed to have the meaning as the equivalent terms are defined in the FADP;

(vi) the list of data subjects and categories of data indicated in Annex I. B. to the SCCs shall not be deemed to restrict the application of the SCCs to the Swiss Personal Data; and

(vii) in all cases the parties satisfy any signature requirement under the FADP by the execution or acceptance of Customer and Omada to the binding Agreement effective between the parties.

(d) **SCC Annex I**:

(i) In respect of Annex I, Section A of the EU SCCs, the requisite information is as follows:

(A) Data exporter(s):

Name: as identified in the Agreement

Address: as identified in the Agreement

Contact person's name, position and contact details: as identified in the Agreement

Activities relevant to the data transferred under these Clauses: <u>For any Omada Identity Subscriptionsoftware</u>: Omada's Support (e.g., program planning, software deployment assistance, interface adapter efforts, and/or formal or non- formal software training).

<u>For Omada Identity Cloud</u>: Omada Identity Cloud, and Support (e.g., implementation services, implementation support, best practices consultations, integration efforts, and training and education services).

Signature and date: the parties agree that any signature requirement is

satisfied by the execution or acceptance of Customer and Omada to the binding Agreement effective between the parties.

Role (controller/processor): Controller

(B) Data importer(s):

Name: Omada

Address:

Contact person's name, position and contact details:

Omada's Data Protection Officer:

dataprotection@omadaidentity.com

Activities relevant to the data transferred under these Clauses:

Same as listed above for data exporter.

Signature and date: the parties agree that any signature requirement is satisfied by the execution or acceptance of Customer and Omada to the binding Agreement effective between the parties.

Role (controller/processor): Processor

(ii) In respect of Annex I, Section B of the EU SCCs, the requisite information is as follows:

(A) Please see Schedule A of the DPA for details of transfer(s);

(B) For transfers to (sub-) processors,

(I) Subject matter of sub-processing:

Identification and contact data (e.g., name, address, title, contact details), employment details (e.g., job title, role, manager), and/or IT information (e.g., entitlements, IP addresses (including IP derived geolocation), usage data, and cookie data) for Customer's employees, contractors, and/or (where licensed under the Agreement) data exporter's business partners and/or end-users authorised by Customer.

(II) Nature of sub-processing:

To assist Omada in providing solutions and other Omada Solution Offering to Customer under the Agreement.

(III) Duration of sub-processing:

The sub-processing will occur for the duration of the processing by Omada in the context of the provision of Omada Solution Offering under the

(iii) In respect of Annex I, Section C of the EU SCCs, the competent supervisory authority shall be the applicable supervisory authority determined under Clause 13 of the EU SCCs.

(e) **SCC Annex II**:

(i) In respect of Annex II of the EU SCCs, the requisite information is as follows:

(A) Description of the technical and organisational measures implemented by the data importer(s)

(I) Application to Transfers

Cross-border transfers by Customer to Omada relate to Omada Solution Offering, including (1) Support for on-premises software and/or (2) Omada Identity Cloud, including Support for Omada Identity Cloud. Customer controls what data Omada has access to for these purposes. As such, Omada's technical and organisational measures, as a whole, concern its access to transferred data.

(II) Technical and Organisational Measures

Please see Schedule B of the DPA, which describes the technical and organisational security measures implemented by Omada.

(B) For transfers to (sub-) processors, Sub-processors shall ensure that they have appropriate technical and organisational measures to protect against and report a personal data breach, appropriate to the harm that might result from such personal data breach, having regard to the state of technological development and the cost of implementing any measures. Such measures may include where appropriate: pseudonymising or encrypting personal data, ensuring Confidential, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after a physical or technical incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it.

4.3 The parties agree that the data export solution identified in Section 4.2 (Standard Contractual Clauses) will not apply if and to the extent that Omada adopts an alternative data export solution for the lawful transfer of Personal Data (as recognised under European Data Protection Laws) outside of the EEA, the UK, or Switzerland in which event, Customer shall take any action (which may include execution of documents) required to give effect to such solution and the alternative transfer mechanism will apply instead (but only to the extent such alternative transfer mechanism extends to the jurisdictions to which Customer Personal Data is transferred.