

Data Privacy Addendum

This Data Privacy Addendum (“**DPA**”) is entered into by and between Ping Identity Limited (“**Ping Identity**”) and the company or entity accepting the DPA (“**Customer**”) and sets forth the parties’ obligations with respect to the Processing of Personal Information (as defined below).

This DPA is incorporated into and forms part of, and is subject to the terms and conditions of, the Agreement (as defined below). If an Affiliate of Customer has executed an ordering document with Ping Identity but is not the original signatory to the Agreement, this DPA is an addendum to and forms part of such ordering documentation. Any capitalized terms used in this DPA and not otherwise defined herein shall have the meanings ascribed to such terms in the Agreement.

1. Definitions

- (a) “**Agreement**” means the subscription or license agreement between Customer and Ping Identity pursuant to which Ping Identity Processes any Personal Information for or on behalf of Customer. “Agreement” encompasses all order forms, statements of work, and/or online terms and conditions between Customer and Ping Identity.
- (b) “**AI Technology**” means any Product or Service (including any feature in such Products or Services) that utilizes machine learning software, algorithms, models, hardware or other artificial intelligence tools or aids to generate information or make predictions, recommendations, or decisions.
- (c) “**CA Privacy Law**” means (collectively) the California Consumer Privacy Act, the California Privacy Rights Act, all implementing regulations, as and when effective, and any other applicable California state privacy laws.
- (d) “**Data Subject Request**” means any request by an individual (or by another person acting on behalf of an individual) to exercise a right under any Privacy Law or any complaint or inquiry about the Processing of the individual’s Personal Information.
- (e) “**Deidentified**” means a data set where (i) all Direct Identifiers have been removed, (ii) individuals cannot reasonably be identified using indirect identifiers in the dataset or using other information available to Ping Identity, and (iii) the data are protected by administrative and technical controls that are reasonably designed to ensure that the data are not re-identified or otherwise used in an identifiable manner. For purposes of this definition, a “Direct Identifier” is any single data element that could reveal a person’s identity, such as a person’s name, username or online identifier, email address, physical address or location, telephone number, device identifier, birthdate or transaction date, identification numbers (such as a government-issued ID number or account number) payment card number, IP address, biometric identifier, photograph or any other image that allows individual identification.
- (f) “**EEA Personal Data**” means that subset of Personal Information consisting of “personal data” (as defined in GDPR) pertaining to residents of the European Economic Area (EEA) and (for convenience) Switzerland and the United Kingdom.
- (g) “**GDPR**” means Regulation (EU) 2016/679 (the General Data Protection Regulation), including as it applies in UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018, and all applicable regulations, as and when effective.
- (h) “**Internal Business Purposes**” means Processing of Personal Information by Ping Identity to (i) make back-ups as part of disaster recovery and business continuity programs; (ii) comply with its own legal or regulatory obligations; (iii) build and improve the quality of the Services, including debugging to identify and repair errors that impair intended functionality, provided that Ping Identity does not use Personal Information to provide services to other companies or to create profiles of individuals (other than for Customer or as needed to mitigate fraud and malicious activity); (iv) confirm usage quantities; and (v) prevent, detect or respond to security incidents or malicious, deceptive, fraudulent, or illegal activity.
- (i) “**Personal Information**” means all data (regardless of format) that (i) identifies or can be used to identify, contact, locate or target a natural person, (ii) pertains in any way to an identified natural person, or (iii) falls within any definition of “personal information” or “personal data” under any applicable Privacy Law, and that is processed by Ping Identity to provide the Services to Customer.
- (j) “**Personal Information Breach**” means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information.

- (k) **“Privacy Laws”** means all applicable laws that regulate the Processing of Personal Information. In particular, the Privacy Laws include (as applicable) the CA Privacy Laws, the GDPR, and other applicable U.S. Federal, state and international laws and regulations that specify privacy, data protection, security or security breach notification obligations or that otherwise regulate the Processing of the Personal Information or the provision of the services by Ping Identity.
- (l) **“Processing”** or **“Process”** means any operation or set of operations which is performed upon Personal Information, whether by automatic means, such as collection, compilation, use, deidentification, disclosure, duplication, organization, storage, alteration, Transfer, transmission, combination, redaction, erasure, or destruction.
- (m) **“Restricted Transfer”** means any Transfer where the applicable Privacy Law requires the parties to demonstrate adequate protection using a standard contractual instrument or other prescribed means. Restricted Transfers do not include Transfers to recipients in countries whose data protection regimes have been declared adequate by relevant data protection authorities, or which are otherwise not restricted.
- (n) **“Services”** means all services Ping Identity provides to or performs for Customer pursuant to the Agreement that entail Processing of Personal Information.
- (o) **“Standard Contractual Clauses”** means (as applicable) (i) the contract terms set forth in the Annex to the European Commission’s decision C(2021) 3972 of 4 June 2021 containing Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, or (ii) other contract terms published by relevant regulatory authorities to authorize data Transfers.
- (p) **“Subprocessor”** means any entity (including an Affiliate of Ping Identity) acting under the instructions of Ping Identity that processes unencrypted Personal Information on behalf of Ping Identity to provide the Services.
- (q) **“Transfer”** means to disclose or otherwise make the Personal Information available to another entity (including to any Ping Identity Affiliate or Subprocessor), either by physical movement of the Personal Information or by enabling remote access to the Personal Information.

2. **General Obligations**

- (a) Each party must use reasonable efforts to stay informed of the legal and regulatory requirements for its applicable responsibilities under this DPA. Ping Identity will comply with those obligations applicable to it as a “data processor” or “service provider,” and Customer will comply with those obligations applicable to it as a “data controller” or “business” (each as defined in the applicable Privacy Laws). Customer shall be responsible for ensuring that it has, and will continue to have, the right to transfer, or provide access to, Personal Information to Ping Identity for Processing as set forth herein. If any authorizations or consents of data subjects are required for such Processing of Personal Information by Ping Identity, Customer shall obtain any such consents directly from the data subjects.
- (b) Ping Identity will only Process Personal Information as needed to provide the Services, as needed for its Internal Business Purposes, as needed to comply with applicable law, or in accordance with Customer’s documented instructions. This DPA, the Agreement, and Customer’s use of the Service’s features and functionality are Customer’s complete set of instructions to Ping Identity in relation to the Processing of Personal Information.
- (c) Customer shall not instruct Ping Identity to Process Personal Information in violation of applicable law. Ping Identity may refuse to comply with any instruction that Ping Identity reasonably believes would violate applicable law. Ping Identity will promptly notify Customer if, in its opinion, the instructions given by Customer for Processing violate any Privacy Law; provided, however, that Ping Identity has no independent obligation to verify that the Processing complies with any specific Privacy Law, as it is entitled to rely on Customer’s instructions.
- (d) The Appendix below contains a description of the Processing activities. Additional information about the Processing activities may be found in the Fact Sheets relevant to the Services that are posted in the Ping Identity Trust Center: <https://www.pingidentity.com/en/legal/privacy-data-processing.html>. Ping Identity may update the Appendix from time to time upon thirty (30) days’ prior written notice to reflect operational, security, product, legal, or Subprocessor changes.
- (e) Unless otherwise prohibited by the Agreement or any applicable Privacy Law, Ping Identity may also further

Process Personal Information as needed to Deidentify it and aggregate it with other customer or third-party data to create datasets for other internal operational purposes such as service improvement, product development, and analytics. Ping Identity will maintain and use Deidentified data in deidentified form and will not attempt to reidentify it. To the extent such data remains subject to Privacy Laws, Ping Identity will continue to Process such data in accordance with this DPA and Privacy Laws.

- (f) Ping Identity will promptly inform Customer in writing: (i) if it cannot comply with any material term of this DPA (if this occurs, Ping Identity will use reasonable efforts to remedy the non-compliance; if Ping Identity cannot remedy it, Customer will be entitled to suspend Ping Identity's Processing of Personal Information); (ii) of any Data Subject Request received by it; (iii) of any other requests with respect to Personal Information received, including (without limitations) of any request for access to any Personal Information received by Ping Identity from any entity, including (without limitation) from any data protection agency, law enforcement agency or pursuant to any civil subpoena, unless it is explicitly prohibited by law from notifying Customer of the request. Ping Identity understands that it is not authorized to respond to these requests without Customer's approval unless the response is legally required under a subpoena or similar legal document issued by a government agency that compels disclosure by Ping Identity.
- (g) Ping Identity will reasonably cooperate with Customer and with its Affiliates and representatives in responding to Data Subject Requests and regulatory inquiries as needed for Customer to demonstrate compliance with the Privacy Laws applicable to it and to respect individuals' rights under such Privacy Laws. Ping Identity will reasonably assist Customer with any data protection impact assessments, cybersecurity audits, automated decision-making requirements, transfer risk assessments or prior consultations with regulators as applicable to Ping Identity's Processing of Personal Information and as needed to comply with the Privacy Laws.

3. Specific Compliance Requirements. To the extent applicable:

- (a) Ping Identity certifies that it will not (i) "sell" the Personal Information or "share" the Personal Information with third parties for online targeting (as those terms are defined in CA Privacy Laws), (ii) retain, use or disclose the Personal Information other than as specified in the Agreement, as needed to perform the Services and for its Internal Business Purposes, (iii) retain, use or disclose the Personal Information outside of its direct business relationship with Customer.
- (b) If the Personal Information includes any Personal Information subject to CA Privacy Laws, Ping Identity will: (i) comply with all applicable sections of CA Privacy Laws, including by providing the same level of privacy protection as required by Customer; (ii) comply with applicable restrictions under CA Privacy Laws on combining the Personal Information with personal information that Ping Identity receives from, or on behalf of, another person or persons, or that Ping Identity collects from any interaction between it and any individual; and (iii) notify Customer if it makes a determination that it can no longer meet its obligations under CA Privacy Laws. Customer shall have the right, upon seven (7) business days' notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information by Ping Identity. More information about Ping Identity's commitment to CA Privacy Law compliance can be found in the Trust Center: <https://www.pingidentity.com/en/legal/ccpa-faqs.html>
- (c) If the Personal Information includes "protected health information" (PHI) as defined in the Privacy, Security and Breach Notification Rules issued under the Health Insurance Portability and Accountability Act ("HIPAA"), the parties agree that the Processing of all such PHI is subject to the existing Business Associate Agreement between Customer and Ping Identity.
- (d) If the Personal Information includes "consumer health data" as defined in an applicable Privacy Law or other sensitive Personal Information or special categories of data, each party shall comply with the specific requirements for the Processing of these data elements that are applicable to the party's respective role (controller/business and processor/service provider). Ping Identity shall restrict access to these data elements to those personnel whose access is needed to provide the Services, and it shall only process these data elements in accordance with Customer's specific binding instructions. Ping Identity shall reasonably assist Customer as needed for Customer to comply with its obligations under applicable Privacy Laws that regulate these data elements.
- (e) Certain Ping Identity products and services incorporate AI Technology to improve usability, security, and fraud detection. Ping Identity uses reasonable and appropriate controls to manage its use of AI Technology and validate that the outputs are free of inappropriate bias, given the purposes for which they are used.

4. Subprocessors

- (a) Ping Identity may subcontract Personal Information to the Subprocessors listed in the Ping Identity Data Supplement (<https://www.pingidentity.com/en/legal/data-supplement.html>) as may be amended by Ping Identity from time to time and Customer may subscribe to receive updates from such website. Prior to a Subprocessor's Processing of Personal Information, Ping Identity will impose contractual obligations on the Subprocessor substantially the same as those imposed on Ping Identity under this DPA. Ping Identity remains primarily liable to Customer for the acts, errors and omissions of the Subprocessor, as if they were Ping Identity's own acts, errors and omissions.
- (b) Ping Identity shall notify Customer of new Subprocessors at least thirty (30) calendar days before authorizing such Subprocessor(s) to Process Personal Information in connection with the provision of the Services. Upon Customer's written request, Ping Identity shall provide copies of relevant Subprocessor agreements. Ping Identity may redact any commercial or confidential information unrelated to the data protection obligations required by this DPA or the Standard Contractual Clauses prior to disclosure.
- (c) Customer may object to a new Subprocessor on reasonable grounds relating to the protection of Personal Information by sending an email to legalnotice@pingidentity.com, within ten (10) business days after receipt of Ping Identity's notice in accordance with Section 4(b). Ping Identity will use commercially reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Information by the objected-to new Subprocessor without unreasonably burdening Customer. If Ping Identity is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may, as its sole and exclusive remedy, terminate its applicable subscriptions from Ping Identity with respect only to those aspects of the Service which cannot be provided by Ping Identity without the use of the new Subprocessor. In such event, Ping Identity shall refund Customer any unused, prepaid Fees for the applicable Service covering the remainder of the subscription term after the date of termination.

5. Data Transfers

- (a) With respect to Ping Identity's hosted service, Customer may select the data center(s) location from those locations offered by Ping Identity in which Personal Information shall be physically stored. Customer understands and agrees that by instructing Ping Identity to use a Subprocessor (such as a data center), the Parties are bound by the Subprocessor's terms and conditions in addition to this DPA.
- (b) Customer authorizes Ping Identity and its Subprocessors to make routine Transfers of Personal Information in accordance with this DPA, Privacy Laws, and approved transfer mechanisms. Ping Identity has certified to the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework, and the UK Extension of the EU-US Data Privacy Frameworks. These certifications provide the primary authorization for Restricted Transfers of EEA Personal Data to Ping Identity in the United States. See: <https://www.dataprivacyframework.gov/s/>. More information about Ping Identity's commitment to GDPR compliance can be found in the Trust Center: <https://www.pingidentity.com/en/legal/gdpr-compliance-faq.html>
- (c) Should any supervisory authority or court determine that any Transfer mechanism used herein is no longer an appropriate basis for Restricted Transfers, Ping Identity and Customer will promptly take all steps reasonably necessary to demonstrate adequate protection for the impacted information, using another approved mechanism. Ping Identity understands and agrees that Customer may terminate the Transfers as needed to comply with the applicable Privacy Laws.
- (d) Should other jurisdictions require specific contractual terms to enable Restricted Transfers, the parties will use good faith efforts to negotiate these instruments as needed to comply with the applicable Privacy Laws. If permitted by law, the parties agree that the terms of the new instruments will be automatically incorporated by reference into this DPA upon either party's circulation of an amendment containing the required transfer terms. The receiving party will have thirty (30) days to object to the amendment by giving the other party written notice, in which case Customer may terminate the Transfers as needed to comply with law.

6. Security and Personal Information Breaches

- (a) Ping Identity has implemented and documented appropriate administrative, technical and physical

measures to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access as described in more detail in the Ping Identity Security Exhibit: <https://www.pingidentity.com/security-exhibit> (the “**Security Exhibit**”). Ping Identity may make future modifications to the measures that do not lower the level of protection of Personal Information.

- (b) Ping Identity may disclose Personal Information to its employees and contingent workers as reasonably needed to provide the Services. Prior to allowing any employee or contingent worker to Process any Personal Information, Ping Identity shall (i) conduct an appropriate background investigation of the individual as permitted by law (and receive an acceptable response), (ii) require the individual to execute an enforceable confidentiality agreement (unless they are subject to a statutory or professional obligation of confidentiality), and (iii) provide the individual with appropriate privacy and security training. Ping Identity will also reasonably monitor its employees and contingent workers for compliance with the privacy and security program requirements.
- (c) Taking into account the nature of Processing and the information available to Ping Identity, Ping Identity will notify Customer without undue delay (and within 72 hours) upon determining that a Personal Information Breach impacts Personal Information. This notification will be made via email to the address specified by Customer in the Appendix. Ping Identity will provide Customer with all information in its possession about the Security Breach reasonably needed by Customer to assess its incident response obligations. Customer is solely responsible for complying with legal requirements for incident notification applicable to Customer and fulfilling any third-party notification obligations related to any Personal Information Breach. Nothing in this DPA shall be construed to require Ping Identity to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Information Breach or other security incidents generally.
- (d) When Ping Identity ceases to perform Services for Customer (and at any other time, upon request), Ping Identity will either (i) return the Personal Information or (ii) purge, delete and destroy the Personal Information. Nothing will oblige Ping Identity to delete or anonymize Personal Information from files created for security, backup and business continuity purposes sooner than required by Ping Identity’s data retention processes. If Ping Identity is required by applicable law to retain any Personal Information, it shall (i) ensure the continued confidentiality and security of the Personal Information, (ii) securely delete or destroy the Personal Information when the legal retention period has expired, and (iii) not actively Process the Personal Information other than as needed for to comply with law.

7. Audit.

- (a) Customer may request that Ping Identity provide it with (i) responses to a reasonable information security-related questionnaire; (ii) copies of Ping Identity’s most recently completed SOC-2 Type II audit report, its public ISO 27001 certificate and non-public Statement of Applicability; (iii) a summary of Ping Identity’s operational practices related to data protection and security; (iv) an executive summary of the most recent annual penetration test; and (v) making Ping Identity’s personnel reasonably available for security-related discussions.
- (b) To the extent required by applicable Privacy Laws, and where the information made available under Section 7(a) is insufficient to demonstrate compliance, Ping Identity will submit its corporate headquarters for a reasonable audit upon at least 30 days prior written notice, not more than once per year, during Ping Identity’s reasonable business hours, which shall be carried out by Customer (or by a qualified independent auditor) in a mutually agreeable manner. In the event a Customer audit takes more than one business day, Customer shall reimburse Ping Identity for any time expended by Ping Identity in fulfilling any such request at Ping Identity’s then-current professional services rates, which shall be made available to Customer upon request. Any independent auditors utilized shall be required to enter into a confidentiality agreement with Ping Identity. For the avoidance of doubt, Customer understands that due to the third-party hosting and multi-tenant nature of the Services, Ping Identity cannot grant access to the premises, facilities, or records of any Subprocessor or Ping Identity’s production or non-production systems, source code, or anything that could expose sensitive information of Ping Identity or the confidential information of other customers of Ping Identity.
- (c) Ping Identity shall also cooperate with any audits conducted by any regulatory agency that has authority over Customer as needed to comply with applicable law.

8. Miscellaneous.

- (a) In the event of a conflict between the terms and conditions of the Agreement and this DPA, this DPA shall control.
- (b) If an amendment to this DPA is required in order to comply with any applicable Privacy Law, the parties will work together in good faith to promptly execute a mutually agreeable amendment to this DPA reflecting the requirements of such Privacy Law.
- (c) Each party's liability arising out of or related to this DPA, whether contract, tort or under any other theory of liability, is subject to any limitation of liability as set forth in the Agreement and any reference to such limitation of liability of a party means the aggregate liability of the party and its Affiliates under the Agreement and this DPA, including its exhibits and attachments, together.
- (d) This DPA shall remain in effect until, and automatically expire upon, deletion of all Personal Information by Ping Identity as described in this DPA.

Appendix to the Data Privacy Addendum
This Appendix also serves as the Appendix to the Standard Contractual Clauses,
if those are used to authorize cross-border data transfers as indicated below.

ANNEX I

A. LIST OF PARTIES

Customer name and address as specified in the Agreement or applicable Order Form.

Customer Contact for Breach Notification: Customer's administrator set forth in Ping Identity's system

Customer acts as the data exporter/controller (or processor acting on behalf of a third-party controller).

and

Ping Identity Limited
4th Floor, Broad Quay House, Prince Street,
Bristol BS1 4DJ, United Kingdom

Ping Identity Privacy Office: privacy@pingidentity.com

Ping Identity acts as the data importer/processor, for itself and its Affiliates, as applicable.

B. DESCRIPTION OF THE PROCESSING AND TRANSFER

Ping Identity provides enterprise identity and access management (IAM) products and related security solutions. Ping Identity's products enable customers to manage and secure access to applications, APIs, systems, and digital services for workforce, consumer, partner, and machine identities. Ping Identity's products range from basic single sign-on solutions to fully orchestrated risk-based, adaptive authentication workflows that support different IAM use cases, such as fraud detection, identity proofing, and authorization.

The Appendix provides a general description of the processing activities. Additional service-specific information regarding data processing activities, hosting, subprocessors, security practices, retention, and categories of personal information (including sensitive personal information, where applicable) may be described in the applicable Ping Identity privacy and data processing fact sheets made available in the Trust Center: <https://www.pingidentity.com/en/legal/privacy-data-processing.html>.

Categories of data subjects whose personal information is processed and/or transferred

Customer's employees, contractors, administrators, end users, consumers, and other natural persons whose personal information is submitted to, collected through, or otherwise processed by Ping Identity in connection with the Services.

Categories of personal information are processed and/or transferred

Customer may submit personal information to the Services, the extent of which is determined and controlled by Customer in its sole discretion. Depending on the Services purchased and Customer's configuration and use of those Services, such personal information may include:

- Identifiers and contact information, such as name, username, email address, postal address, phone number, and similar account or internal identifiers (e.g., employee ID, user ID)
- Professional or employment-related information, such as employer, title, and manager
- Authentication, security, and access-related information, such as security questions and answers, MFA enrollment details, authentication events, session information, access privileges, and authorization history
- Device, network, and technical information, such as IP address, device identifiers, connection data, and localization data
- Behavioral or fraud-related signals, such as keystroke dynamics and similar signals used for fraud or bot detection and not for individual identification
- Additional categories of personal information processed or stored through configurable features, including orchestration, directory, or workflow functionality, which are determined by Customer and are not required by Ping Identity.

Sensitive personal information processed and/or transferred (if applicable)

Ping Identity's Services generally do not require the processing of special categories of personal data or sensitive personal information. However, certain Services may enable or support the processing of such data where configured, enabled, or otherwise instructed by Customer.

The categories of sensitive personal information processed, if any, depend on the specific Services purchased and Customer's configuration and use of those Services. Additional service-specific information regarding sensitive personal information processing is further described, where applicable, in the relevant Ping Identity privacy and data processing fact sheets made available in the Trust Center:

<https://www.pingidentity.com/en/legal/privacy-data-processing.html>.

For example:

- certain identity verification or authentication features may involve the processing of biometric data or government-issued identification information where enabled or implemented by Customer; and
- certain orchestration, directory, or workflow functionality may permit Customer to submit or process additional categories of personal information, including sensitive personal information or special categories of personal data, which are determined and controlled by Customer and are not required by Ping Identity for general service functionality.

Nature of the processing

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

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

Personal information will be retained by the data importer in accordance with its data retention policy and no longer than necessary for the purposes set forth in the Agreement.

Physical location of personal information

For hosted solutions, Customer will select the data center(s) from those locations offered by Ping Identity.

Purpose(s) of the data transfer and further processing

To enable Ping Identity to provide the IAM products and services per the Agreement.

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

Continuous

C. COMPETENT SUPERVISORY AUTHORITY FOR RESTRICTED TRANSFERS

Restricted Transfer	Competent Supervisory Authority & Governing Law
EEA Transfers – per Schedule 1	Schleswig-Holstein DPA (Germany)
Swiss Transfers	Federal Data Protection & Information Commissioner (FDPIC) – Switzerland
UK Data Transfers – per Schedule 2	Information Commissioner (ICO) – United Kingdom

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

Ping Identity's information security program is described here: <https://www.pingidentity.com/security-exhibit>.

ANNEX III – LIST OF SUBPROCESSORS

Customer has authorized Ping Identity's use of the subprocessors listed here:

<https://www.pingidentity.com/en/legal/data-supplement.html>