DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Agreement between SailPoint and Customer and shall be effective on the effective date of the Agreement ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

1.1. The following terms shall have meanings ascribed for the purposes of this DPA:

"**Affiliate**" has the meaning set forth in the Agreement, or if no such meaning is given, means an entity that controls, is controlled by or shares common control with a party, where such control arises from either (i) a direct or indirect ownership interest of more than 50% or (ii) the power to direct or cause the direction of the management and policies, whether through the ownership of voting stock by contract, or otherwise, equal to that provided by a direct or indirect ownership of more than 50%.

"**Agreement**" means an agreement in effect between Customer and SailPoint that governs Customer's use of, and SailPoint's provision to Customer of, specific SailPoint Offerings.

"**Customer**" means the party identified in the applicable Agreement in effect between SailPoint and such party.

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

"**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.

"**Marketplace**" means an online marketplace operated or controlled by a third party, which is authorised to market and/or distribute SailPoint Offerings.

"**Order**" means SailPoint's quote, statement of work, or an ordering document (including online order form) accepted by Customer through either: (i) Customer's signature on the SailPoint or Partner quote; or (ii) the issuance of a purchase order or other ordering document submitted to SailPoint (directly or indirectly through a Partner or Marketplace) to order the SailPoint Offerings on Customer's behalf, which references the SailPoint Offering, pricing and other applicable terms set forth in an applicable SailPoint quote or ordering document. Orders do not include any preprinted terms on a Customer purchase order or other terms on a purchase order that are inconsistent with or additional to the terms of the Agreement.

"**Other Services**" means, collectively or individually, all technical and non-technical consulting and advisory services identified in an Order as Professional Services (which may be identified as "Setup Services" or "Expert Services") or Training Services purchased by Customer and performed or delivered by SailPoint under the Agreement. For purposes of clarity, "Other Services" does not include the SaaS Services, or Support.

"**Personal Information**" 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.

"**Partner**" means a third party that has an agreement with SailPoint that authorises the third party to resell specific SailPoint Offerings and Other Services to Customer.

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

"**Professional Services**" means consulting services provided by SailPoint to Customer that support Customer's deployment, extension and use of SailPoint Offerings and include, but are not limited to, implementation services, implementation support, best practices consultations, and integration efforts as further described in, and subject to, the Agreement (including the applicable Order).

"**SaaS Services**" means any internet-accessible software-as-a-service offering hosted by SailPoint, its Affiliates or SailPoint's or its Affiliates' service providers, that has been purchased for Customer's use under an Order and made available to Customer over a network.

"**SailPoint Offerings**" means any Software and Services made available or otherwise provided by SailPoint to Customer.

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

"**Services**" means services provided by SailPoint to Customer which may include: (i) SaaS Services; (ii) Support; and (iii) Other Services provided by SailPoint to Customer pursuant to the Agreement.

"**Software**" means the object code version of the specific SailPoint computer software licensed to Customer under an Order, including any updates, modifications, new versions or releases.

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

"**Support**" means SailPoint's support and maintenance services for SailPoint Offerings as described in, and provided in accordance with the SailPoint Support Policy: at https://www.sailpoint.com/legal/.

"**Training Services**" means SailPoint's courses and other product-related training available through SailPoint's Identity University, on-site at SailPoint's, Customer's or a third party's location, or online via a SailPoint-provided website, as agreed by the parties.

1.2. Capitalised 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.

2. Jurisdiction-Specific Addenda

2.1. Attached to this DPA are Addenda that provide terms specific to the Processing of Customer Personal Information arising out of specific legal requirements from particular jurisdictions. In the event that Customer Personal Information 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 soley with respect to Customer Personal Information 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 Information from the relevant jurisdiction shall control with respect to Customer Personal Information from that relevant jurisdiction, and solely with regard to the portion of the provision in conflict.

2.2. Attached to this DPA is the United States Privacy Law Addendum as Schedule B and the European Addendum as Schedule C. In the event Customer believes Customer Personal Information 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 SailPoint and working with SailPoint to effectuate such Addenda. Such additional Addenda shall apply subject to the requirements of this Section 2.

3. Updates to DPA

3.1. When Customer renews or purchases SailPoint Offerings or Professional Services, the then-current DPA terms will apply during the term of the Order for such SailPoint Offerings or Professional Services.

3.2. 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, SailPoint 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.

4. Roles and Scope of Processing

4.1. **Customer Processing of Personal Information.** Customer: (i) agrees that it will comply with its obligations under Data Protection Laws in respect of its Processing of Personal Information and any Processing instructions it issues to SailPoint; 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 SailPoint to Process Personal Information and provide the Services pursuant to the Agreement and this DPA.

4.2. **Customer Instructions.** SailPoint will Process Customer Personal Information only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions and applicable Data Protection Laws. SailPoint will not Process Customer Personal Information provided by or collected on behalf of Customer for any purpose except as necessary to maintain or provide the Services specified in the Agreement and this DPA, or as necessary to comply with the law or binding order of a governmental body. In the event that SailPoint has a legal obligation to Process the Customer Personal Information, SailPoint will notify the Customer of this obligation unless it is legally prohibited from doing so. The parties agree that this DPA, including all applicable Addenda, and the Agreement set out the Customer's complete instructions to SailPoint in relation to the Processing of Customer Personal Information by

SailPoint. Additional Processing outside the scope of these instructions (if any) will require prior written agreement between Customer and SailPoint.

4.3. Details of Data Processing.

(a) Categories of data subjects whose Personal Information is transferred:

Customer's employees, contractors, and/or (where licensed under the Agreement) data exporter's business partners and/or end-users authorised by Customer.

(b) Categories of Personal Information transferred:

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, usage data, cookies data, and geolocation).

(c) Sensitive data transferred (if applicable):

None.

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

For Support and Other Services: one-off. Customer controls what information (including Personal Information) it shares with SailPoint and when it shares such information (including Personal Information) in the context of the provision of ancillary support and account administration services under the Agreement.

For SaaS Services: continuous. Customer controls what information (including Personal Information) it shares with SailPoint and what systems it connects to the SaaS Services. The SaaS Services may allow for a one-off data transfer or connectivity to facilitate transfer on a regularly scheduled and/or continuous basis. Customer determines its configuration and use of the SaaS Services under the Agreement.

(e) Nature of the processing

To provide Services to Customer under the Agreement.

(f) Purpose(s) of the data transfer and further processing

The provision of Services by SailPoint under the Agreement.

(g) The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period

The Customer Personal Information Processed by SailPoint will be retained for the duration of the Processing by SailPoint in the context of the provision of Services under the Agreement, and thereafter in order to comply with applicable law, including Data Protection Laws. Should the Customer make a request to have continued access to its Customer Personal Information, SailPoint will, after a recovery period of up to 30 days following such expiry or termination, comply with this instruction as soon as reasonably practicable, where technically feasible. Customer shall be responsible for retrieving any remaining Customer Personal Information it wishes to retain before the end of the recovery period. SailPoint shall not be required to delete or return Customer Personal Information to the extent: (i) SailPoint is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Personal Information; and/or (ii), Customer Personal Information it has archived on back-up systems, which Customer Personal Information SailPoint shall securely isolate and protect from any further processing, except to the extent required by applicable law.

4.4. Customer Personal Information for Support. Customer acknowledges that SailPoint does not ordinarily require the Processing of Customer Personal Information on Customer's behalf to resolve a technical issue for Support. Customer shall use commercially reasonable efforts to minimize any transfer of Customer Personal Information to SailPoint for Support purposes. Such efforts shall include, but not be limited to, removing, anonymizing and/or pseudononymizing Customer Personal Information in files submitted to SailPoint in a Support request prior to any Processing by SailPoint, in each case to the extent such removal, anonymization and/or pseudononymization is reasonably practicable under the circumstances.

5. Sub-processing

5.1. Authorised Sub-processors. Customer understands and hereby authorises SailPoint to engage Sub-processors to Process Customer Personal Information on Customer's behalf as listed on SailPoint's website at https://www.sailpoint.com/legal/sub-processors.

5.2. Sub-processor Obligations. SailPoint will: (i) not engage a Sub-processor unless SailPoint 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; and (ii) remain responsible for its compliance with the obligations of this DPA and for

any failure by a Sub-processor engaged by SailPoint to fulfil its data protection obligations under the applicable Data Protection Laws.

6. Security

6.1. **Security Measures**. Taking into account the nature of the Processing, SailPoint shall implement and maintain reasonable technical and organisational security measures to protect Customer Personal Information from Security Incidents and to preserve the security and confidentiality of the Customer Personal Information, in accordance with SailPoint's security standards described in **Schedule A**, as applicable to the Services ("**Security Measures**").

6.2. **Updates to Security Measures**. Customer is responsible for reviewing the information made available by SailPoint relating to the Security Measures and making an independent determination as to whether such Security Measures meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that SailPoint may update or modify the Security Measures from time-to-time provided that such updates and modifications do not result in a material degradation of the overall security of the Services.

6.3. **Customer Responsibilities**. Customer agrees that, without prejudice to SailPoint's obligations under Section 6.1 (Security Measures) and Section 9.2 (Security Incident Response):

(a) Customer is responsible for its use of the Services, including: (i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Information;(ii) securing its account authentication credentials; (iii) protecting the security of Customer Personal Information when in transit to and from the Services; (iv) taking appropriate steps to securely encrypt and/or backup any Customer Personal Information uploaded to the Services; and (v) properly configuring the Services and using available features and functionalities to maintain appropriate security in light of the nature of the Customer Personal Information Processed as a result of Customer's use of the Services; and

(b) SailPoint has no obligation to protect Customer Personal Information that Customer elects to store or transfer outside of SailPoint's and its Sub-processors' (where applicable) systems (for example, offline or on-premises storage).

7. Security Reports and Audits

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

7.2. If Customer reasonably believes that the Report provided is insufficient to demonstrate compliance with this DPA, SailPoint shall also provide written responses (on a confidential basis) to reasonable requests for information made by Customer related to its Processing of Customer Personal Information, including responses to information security and audit questionnaires that are reasonably necessary to demonstrate SailPoint's compliance with this DPA, provided that Customer shall not be permitted to exercise this right more than once every 12 months.

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

8. **International Operations**. SailPoint may store and Process Customer Personal Information in any countries where SailPoint, its Affiliates or its Sub-processors maintain data processing operations. SailPoint Affiliates and Sub-processors are listed on SailPoint's website at https://www.sailpoint.com/legal/sub-processors.

9. Additional Security

9.1. **Confidentiality of Processing**. SailPoint shall ensure that any person who is authorised by SailPoint to Process Customer Personal Information (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

9.2. **Security Incident Response**. SailPoint shall: (i) taking into account the nature of SailPoint's Processing of Customer Personal Information and the information available to SailPoint, 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; and (iii) promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.3. **Notification**. Customer acknowledges that SailPoint will not assess the contents of Customer Personal Information 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.

10. Relationship with the Agreement

10.1. 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 Information.

10.2. 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 SailPoint 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 SailPoint's liability under the Agreement as if it were liability to the Customer under the Agreement.

10.3. Any claims against SailPoint or its Affiliates under this DPA shall only be brought by the Customer entity that is a party to the Agreement against the SailPoint 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.

10.4. 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.

10.5. This DPA will terminate automatically with the termination or expiry of the Agreement, subject to additional provisions in any Addenda attached hereto.

Schedule A – Security Measures

SailPoint Data Security Program

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

1. Security Program

a. **ISO27001-based Information Security Management System (ISMS)**: SailPoint shall maintain an ISMS risk-based security program to systematically manage and protect the organisation's business information and the information of its customers and partners.

b. **Security Governance Committee**: SailPoint shall maintain a security committee comprised of leaders across all business units that oversees the company's security program. This committee shall meet monthly to review the operational status of the ISMS (including risks, threats, remediation actions, and other security-related issues) and drive continuous security improvement throughout the business.

c. **Security incident response policy**: SailPoint shall maintain policies and procedures to (1) investigate and respond to security incidents, including procedures to assess the threat of relevant vulnerabilities or security incidents using defined incident classifications and categorisations and (2) establish remediation and mitigation actions for events, including artifact and evidence collection procedures and defined remediation steps.

d. **Policy maintenance**: All security and privacy related policies shall be documented, reviewed, updated and approved by management at least annually to ensure they remain consistent with best practices, legal and regulatory requirements and industry standards.

e. **Communication and commitment**: Security and privacy policies and procedures shall be published and effectively communicated to all personnel and relevant subcontractors. Security shall be addressed at the highest levels of the company with executive management regularly discussing security issues and leading company-wide security initiatives.

2. Personnel Security

a. **Background screening**: Personnel who have access to Customer Personal Information or the equipment on which it is stored shall be subject to background screening (as allowed by local laws and regulations) that shall include verification of identity, right to work and academic degrees and a check of criminal records, sex offender registries and prohibited/denied party lists.

b. **Confidentiality obligations**: Personnel who have access to Customer Personal Information shall be subject to a binding contractual obligation with SailPoint to keep the Customer Personal Information confidential.

c. **Security awareness training**: Personnel shall receive training upon hire and at least annually thereafter covering security best practices and privacy principles.

d. **Code of conduct**: SailPoint shall maintain a code of business conduct policy and compliance program to ensure ethical behavior and compliance with applicable laws and regulations.

3. Third-Party Security

a. **Screening**: SailPoint shall maintain policies and procedures to ensure that all new suppliers, SaaS applications, IT Software, and IT service solutions are subject to reasonable due diligence to confirm their ability to meet corporate security and compliance requirements as well as business objectives.

b. **Contractual obligations**: SailPoint shall ensure that contractual agreements with suppliers include confidentiality and privacy provisions as appropriate to protect SailPoint's interests and to ensure SailPoint can meet its security and privacy obligations to customers, partners, employees, regulators and other stakeholders.

c. **Monitoring**: SailPoint shall periodically review existing third-party suppliers to ensure the supplier complies with contractual terms, including any security and availability requirements. The monitoring program shall review suppliers at least annually (regardless of length of contractual term) to confirm that the supplier/solution is still meeting the company's objectives and the supplier's performance, security, and compliance postures are still appropriate given the type of access and classification of

data being accessed, controls necessary to protect data, and applicable legal and regulatory requirements.

4. Physical Security

a. **Corporate facility security**: A facility security program shall be maintained that manages building entrances, CCTVs, and overall security of its offices, including a security perimeter (including barriers such as card controller entry gates or manned reception desks). All employees, contractors and visitors shall be required to wear identification badges which distinguish their respective role.

b. **Corporate data center security**: Systems installed on SailPoint's premises and used to Process Customer Personal Information shall be protected in such a manner that unauthorised logical or physical access is effectively prevented; equipment used to Process Customer Personal Information cannot be moved, removed, upgraded or reconfigured without appropriate authorisation and protection of the information; and, when equipment Processing Customer Personal Information is decommissioned, Customer Personal Information shall be disposed of securely in a manner that would prevent its reconstruction.

c. **SaaS Services data center security**: SailPoint leverages Infrastructure as a Service (IaaS) data centers for hosting the SaaS Services. SailPoint assesses the security and compliance measures of the applicable data center providers, and the providers follow industry best practices and comply with numerous standards.

5. Solution Security

a. **Software development life cycle (SDLC)**: SailPoint shall maintain a software development life cycle policy that defines the process by which personnel create secure products and services and the activities that personnel must perform at various stages of development (requirements, design, implementation, verification, documentation and delivery).

b. **Secure development**: Product management, development, test and deployment teams shall follow secure application development policies and procedures that are aligned to industry-standard practices, such as the OWASP Top 10.

c. **Vulnerability assessment**: SailPoint shall regularly conduct risk assessments, vulnerability scans and audits (including third-party penetration testing of the SaaS Services twice annually and software upon each new version release). Identified product solution issues shall be scored using the Common Vulnerability Scoring System (CVSS) risk-scoring methodology based on risk impact level and the likelihood and potential consequences of an issue occurring. Vulnerabilities are remediated on the basis of assessed risk. Upon request from Customer, SailPoint shall provide information about the identified vulnerabilities and the measures taken to remediate or address any such vulnerabilities.

6. Operational Security

a. Access controls: SailPoint shall maintain policies, procedures, and logical controls to establish access authorisations for employees and third parties to limit access to properly authorised personnel and to prevent unauthorised access. Such controls shall include:

i. requiring unique user IDs to identify any user who accesses systems or data;

ii. managing privileged access credentials in a privileged account management (PAM) system;

iii. communicating passwords separately from user IDs;

iv. ensuring that user passwords are (1) changed at regular intervals; (2) of sufficient length and complexity; (3) stored in an encrypted format; (4) subject to reuse limitations; and (5) not assigned to other users, even at a different time; and

v. automatically locking out users' IDs when a number of erroneous passwords have been entered.

b. **Least privilege**: SailPoint shall ensure that personnel only have access to systems and data as required for the performance of their roles; only authorised personnel have physical access to infrastructure and equipment; access to production resources for the SaaS Services is restricted to employees requiring access; and access rights are reviewed and certified at least annually to ensure access is appropriate.

c. **Malware**: SailPoint shall utilise industry-standard measures to detect and remediate malware, viruses, ransomware, spyware, and other intentionally harmful programs that may be used to gain unauthorised access to information or systems.

d. **Encryption**: SailPoint shall use industry-standard strong encryption methods to protect data in transit and at rest as appropriate to the sensitivity of the data and the risks associated with loss; all laptops

and other removable media, including backup tapes, on which Customer Personal Information is stored shall be encrypted.

e. **Business continuity and disaster recovery (BCDR)**: SailPoint shall maintain formal BCDR plans that are regularly reviewed and updated to ensure SailPoint's systems and services remain resilient in the event of a failure, including natural disasters or system failures.

f. **Data backups**: SailPoint shall backup data and systems using alternative site storage available for restore in case of failure of the primary system. All backups shall use strong encryption in transit and at rest.

g. **Change management**: SailPoint shall maintain change management policies and procedures to plan, test, schedule, communicate, and execute changes to SailPoint's SaaS Services infrastructure, systems, networks, and applications.

h. **Network security**: SailPoint shall implement industry standard technologies and controls to protect network security, including firewalls, intrusion prevention systems, monitoring, network segmentation, VPN and wireless security. Networks shall be designed and configured to restrict connections between trusted and untrusted networks, and network designs and controls shall be reviewed at least annually.

i. **Data segregation**: SailPoint shall implement logical controls, including logical separation, access controls and encryption, to segregate Customer's Personal Information from other customer and SailPoint data in the SaaS Services. SailPoint shall additionally ensure that production and non-production data and systems are separated.

Schedule B - United States Privacy Law Addendum

This United States Privacy Law Addendum ("**US Addendum**") supplements the DPA and includes additional information required by the CPRA and VCDPA (each as defined below). 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 Scope

(a) This Section 1 shall apply in the event that SailPoint Processes Customer Personal Information of California residents.

1.2 Definitions

(a) The California Consumer Privacy Act is Cal. Civ. Code § 1798.100, et seq. as amended by the California Privacy Rights Act ("**CPRA**"), as may be amended from time-to-time, and any accompanying legally binding regulations that are promulgated to address provisions in the CPRA.

(b) For purposes of this Section 1, the terms "**Business**," "**Business Purpose**," "**Commercial Purpose**," "**Consumer**," "**Personal Information**," "**Processing**," "**Sell**," "**Service Provider**," "**Share**," and "**Verifiable Consumer Request**" shall have the meanings set forth in the CPRA.

(c) All references to "**Personal Information**," "**Controller**," "**Processor**," and "**Data Subject**" in the DPA shall be deemed to be references to "**Personal Information**," "**Business**," "**Service Provider**," and "**Consumer**" as defined in the CPRA.

1.3 Terms

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

(b) Customer will disclose Personal Information to SailPoint only for the limited and specified purposes described in Section 4.3 of the DPA.

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

(d) SailPoint will not retain, use, or disclose Customer Personal Information 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 CPRA.

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

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

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

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

(i) In the event that SailPoint engages a new Sub-processor to assist SailPoint in providing the Services to Customer under the Agreement, SailPoint will (i) notify Customer, in writing, of any intended additional or replacement Sub-processor who will Process Customer Personal Information at least thirty (30) days prior to when the Sub-processor begins Processing Customer Personal Information; and (ii) enter into a written contract with the Sub-processor requiring Sub-processor to observe all of the applicable requirements set forth in the CPRA.

1.4 Consumer Rights

(a) Taking into account the nature of the Processing, SailPoint shall (at Customer's request and expense) provide reasonable cooperation to assist Customer to respond to Verifiable Consumer Requests to exercise the Consumer's rights under the CPRA, where possible, provided that (i) Customer is itself unable to respond without SailPoint's assistance and (ii) SailPoint is able to do so in accordance with all applicable laws, rules, and regulations. In the event that any request from consumers or applicable regulatory authorities is made directly to SailPoint, SailPoint will not respond to such communication directly without Customer's prior authorisation other than to inform the requestor that SailPoint is not authorised to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to do so, and instead, after being notified by SailPoint, Customer will respond. If SailPoint is required to respond to such a request, SailPoint will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so. Customer is solely responsible for ensuring that Consumer requests are communicated to SailPoint, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Consumer.

(b) If a law enforcement agency sends SailPoint a demand for Customer Personal Information (e.g., a subpoena or court order), SailPoint will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, SailPoint may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Information to a law enforcement agency, then SailPoint will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent SailPoint is legally permitted to do so.

1.5 Audit Rights

(a) To the extent required by the CPRA, SailPoint will allow Customer to conduct inspections or audits in accordance with Section 7 of the DPA.

2. VIRGINIA

2.1 Scope

(a) This Section 2 shall apply in the event that SailPoint Processes Customer Personal Information of Virginia residents.

2.2 Definitions

(a) The Virginia Consumer Data Protection Act is Va. Code §§ 59.1-575 et seq. ("**VCDPA**"), as may be amended from time-to-time, and any accompanying legally binding regulations that are promulgated to address provisions in the law.

(b) For purposes of this Section 2, the terms "**Consumer**," "**Controller**," "**Personal Data**," "**Processing**," and "**Processor**" shall have the meanings set forth in the VCDPA.

(c) For purposes of this Section 2, all references to "**Data Subject**" in this DPA shall be deemed to be references to "**Consumer**" as defined in the VCDPA.

2.3 Obligations

(a) The parties acknowledge and agree that Customer is a Controller and SailPoint is a Processor for the purposes of the VCDPA (to extent it applies).

(b) The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Section 4.3 of the DPA.

(c) SailPoint shall adhere to Customer's instructions with respect to the Processing of Customer Personal Data and shall assist Customer in meeting its obligations under the VCDPA by:

(i) taking into account the nature of the Processing, at Customer's request and expense, providing reasonable cooperation to assist Customer to respond to Consumer rights requests where possible, provided that (i) Customer is itself unable to respond without SailPoint's assistance and (ii) SailPoint is able to do so in accordance with all applicable laws, rules, and regulations. In the event that any request from consumers or applicable regulatory authorities is made directly to SailPoint, SailPoint will not respond to such communication directly without Customer's prior authorisation other than to inform the requestor that SailPoint is not authorised to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to do so, and instead, after being

notified by SailPoint, Customer will respond. If SailPoint is required to respond to such a request, SailPoint will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so. Customer is solely responsible for ensuring that Consumer requests are communicated to SailPoint, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Consumer.

(ii) Complying with Section 6 ("Security") of the DPA with respect to Personal Data provided by Customer;

(iii) In the event of a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Personal Data, providing information sufficient to enable Customer to meet its obligations pursuant to Va. Code § 18.2-186.6; and

(iv) Providing information sufficient to enable Customer to conduct and document data protection assessments to the extent required by VCDPA.

(d) SailPoint shall maintain the confidentiality of Personal Data provided by Customer and require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;

(e) Upon Customer's written request, SailPoint shall delete or return all Personal Data provided by Customer, unless retention of such Personal Data is required or authorised by law or the DPA and/or Agreement.

(f) In the event that SailPoint engages any new Sub-processor to assist SailPoint in providing the Services to Customer under the Agreement, SailPoint shall enter into a written contract with the Sub-processor requiring Sub-processor to observe all of the applicable requirements of a Processor set forth in the VCDPA.

2.4 Audit Rights

(a) Upon Customer's written request at reasonable intervals, SailPoint shall, as set forth in Section 7 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate SailPoint's compliance with its obligations under the VCDPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the VCDPA.

Schedule C - 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) SailPoint Processes Customer Personal Information 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.

2. Definitions

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

2.2 "**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 SailPoint Processes any Personal Information 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 SailPoint Processes any Personal Information 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.

2.3 "**SCCs**" means, collectively, (i) where Personal Information 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 Information 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 5 below.

2.4 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. Sub-processors.

3.1 SailPoint's list of Sub-processors is located on SailPoint's website at https://www.sailpoint.com/legal/sub-processors.

3.2 In respect of Clause 9(a) of the SCCs:

(a) SailPoint shall notify Customer, in writing, of any intended additional or replacement Sub-processor who will Process Customer Personal Information at least thirty (30) days prior to when the Sub-processor begins Processing Customer Personal Information (such period, the "**Review Period**");

(b) Customer may object to any additional or replacement Sub-processor at any time during the Review Period. Any objections raised by Customer during the Review Period may only be based on reasonable grounds and only with respect to data protection concerns;

(c) Customer may object to SailPoint's additional or replacement Sub-processor by providing notice of Customer's objection, in writing, and in the manner provided in the Agreement. SailPoint will have a reasonable time to notify Customer, in writing, that the proposed addition or replacement shall not apply to any of the Services provided by SailPoint to the Customer or allow the Customer to terminate for convenience the affected Services used by Customer, and in the manner provided in the Agreement. Customer will continue to pay all fees for the affected Services until the termination takes effect, and SailPoint will refund Customer on a pro-rated basis any unused and prepaid fees covering the remainder of the term of the terminated Agreement following the effective date of termination; and

(d) 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 Services after the Review Period has lapsed. CLAUSE 9(A) OF THE SCCS AND THIS SECTION 3.2 STATE THE ENTIRE LIABILITY OF SAILPOINT 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. Cooperation

4.1 Taking into account the nature of the Processing, SailPoint shall (at Customer's request, cost, and expense) provide reasonable cooperation to assist Customer to respond to any requests from data subjects in relation to their data subject rights under European Data Protection Laws or applicable regulatory authorities relating to the Processing of Customer Personal Information under the Agreement.

4.2 If a law enforcement agency sends SailPoint a demand for Customer Personal Information (e.g., a subpoena or court order), SailPoint will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, SailPoint may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Information to a law enforcement agency, then SailPoint will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent SailPoint is legally permitted to do so.

4.3 In the event that any request from data subjects or applicable regulatory authorities is made directly to SailPoint, SailPoint shall not respond to such communication directly without Customer's prior authorisation other than to inform the requestor that SailPoint is not authorised to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to reply. Customer shall bear the responsibility for responding to all such requests.

4.4 If SailPoint is legally required to respond to a request enumerated in Sections 4.2 and 4.3, SailPoint will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

4.5 Customer acknowledges that SailPoint 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 SailPoint 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 Information, Customer will, where requested, provide such information to SailPoint, and will ensure that all information provided is kept accurate and up-to-date.

4.6 Taking into account the nature of the Processing and information available to SailPoint, SailPoint shall (at Customer's request and expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments.

5. Standard Contractual Clauses

5.1 To the extent that SailPoint Processes any Customer Personal Information from the EEA, the UK, or Switzerland, and transfers such Customer Personal Information 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 SailPoint (as "data importer") as follows:

(a) **EU Personal Information**. In respect of Personal Information 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 3 (Sub-processors) of the European Addendum;

(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 SailPoint to the binding Agreement effective between the parties.

(b) **UK Personal Information**. In respect of Personal Information 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 5.1(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 5.1(a) of the European Addendum;

(iii) Table 3 of the UK SCCs is completed with the relevant information in Sections 5.1(d) and 5.1(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 SailPoint to the binding Agreement effective between the parties.

(c) **Swiss Personal Information**. In respect of Personal Information that is protected by the FADP, the EU SCCs as completed in Section 5.1(a) will apply for any Restricted Transfers, are incorporated by reference, and are amended as follows:

(i) the term "personal data" or "personal information" shall be deemed to include information relating to an identified or identifiable legal entity;

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

(iii) 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**");

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

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

(vi) 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;

(vii) 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 Information; and

(viii) in all cases the parties satisfy any signature requirement under the FADP by the execution or acceptance of Customer and SailPoint 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:
For any on-premises software: SailPoint's Support and Other Services (e.g., program planning, software deployment assistance, interface adapter efforts, and/or formal or non-formal software training).
For any SaaS solutions: SailPoint's SaaS Services, Support, and Other Services (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 SailPoint to the binding Agreement effective between the parties.
Role (controller/processor): Controller

(B) Data importer(s):

Name: SailPoint Technologies, Inc.
Address: 11120 Four Points Drive, Suite 100, Austin, Texas 78726, USA
Contact person's name, position and contact details:
SailPoint's Data Protection Officer:
Dr. Felix Wittern
Partner, Fieldfisher
Hamburg, Germany
privacy@sailpoint.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 SailPoint 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 Section 4.3 (Details of Data Processing) 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, usage data, cookies data, and geolocation) 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 SailPoint in providing solutions and other Services to Customer under the Agreement.

(III) Duration of sub-processing:

The sub-processing will occur for the duration of the processing by SailPoint in the context of the provision of Services under the Agreement unless SailPoint earlier terminates and/or replaces the sub-processor.

(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 SailPoint relate to SailPoint's (1) support and maintenance services for on-premises software and/or (2) SaaS Services and professional services. Customer controls what data SailPoint has access to for these purposes. As such, SailPoint's technical and organisational measures, as a whole, concern its access to transferred data.

(II) Technical and Organisational Measures

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

(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 confidentiality, 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.

5.2 The parties agree that the data export solution identified in Section 5.1 (Standard Contractual Clauses) will not apply if and to the extent that SailPoint adopts an alternative data export solution for the lawful transfer of Personal Information (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 Information is transferred).