SOFTWARE AS A SERVICE AGREEMENT EMEA (V.20210212)

PLEASE READ THIS SAAS AGREEMENT BEFORE USING SAILPOINT'S SERVICES. BY ACCESSING OR USING SAILPOINT'S IDENTITY NOW SOFTWARE AS A SERVICE OFFERING, YOU ("the Customer") SIGNIFY ACCEPTANCE OF AND AGREE TO THE TERMS AND CONDITIONS OF THIS SAAS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS SAAS AGREEMENT, DO NOT ACCESS OR USE THE SERVICES. IF THE PARTIES HAVE A FULLY EXECUTED AGREEMENT THAT EXPRESSLY GOVERNS ORDERS FOR SAILPOINT'S SOFTWARE AS A SERVICE OFFERING, SUCH AGREEMENT SHALL SUPERSEDE THIS SAAS AGREEMENT.

WHEREAS, SailPoint is the provider of SaaS Service and the Customer wishes to obtain access to the same under the terms of this SaaS Agreement; and

WHEREAS, the parties desire that this SaaS Agreement serve as a master agreement between them for the purposes of any Orders that Customer may place with SailPoint or a Partner, from time to time.

1. DEFINITIONS

As used in this SaaS Agreement:

"**Customer Data**" means all data and other information that Customer or a User provides or makes available to SailPoint in connection with the Services or this SaaS Agreement.

"**Customer Personal Data**" means all Customer Data relating to an identified or identifiable natural person.

"**Documentation**" means the user guides, online help, and release notes, provided or made available by SailPoint to Customer regarding the use or operation of the SaaS Service.

"**DPA**" means the provisions detailed in the SaaS Customer Data Processing Addendum attached hereto as Exhibit A.

"**Identity Cube**" means a unique collection of identity data for an individual human, a non-human bot, or other user that will be granted access to and/or managed by the SaaS Service. Identity data may be physically or logically maintained in a single repository or in separate physical or logical repositories.

"**Order**" means the schedule, quotation, statement of work, or other document(s) by which Customer orders the SaaS Service or Other Services pursuant to this SaaS Agreement.

"**Other Services**" means all technical and non-technical services identified in an Order and performed or delivered by SailPoint under this SaaS Agreement, consisting solely of implementation services, implementation support, best practices consultations, integration efforts, and training and education services, which are provided on a non-work for hire basis and documented in statements of work mutually agreed to by the parties. For purposes of clarity, Other Services does not include the SaaS Service or the SaaS Support.

"**Partner**" means a reseller or distributor that has an agreement with SailPoint that authorises them to resell the SaaS Service or Other Services.

"**Required Software**" means the object code version of the Virtual Appliance, including any updates or new versions. The Required Software is a virtual machine that connects Customer's target Sources using public APIs, connectors, and integrations to the SaaS Service.

"**SaaS Service**" means the specific SailPoint internet-accessible identity governance software-as-a-service(s) identified in an Order hosted by SailPoint or its service provider and made available to Customer over a network on a term-use basis and, except with respect to Section 2.1 (Provision of SaaS Service), includes the Required Software.

"**Services**" means the SaaS Service, SaaS Support, and Other Services.

"**Source**" means a Customer managed target system for reading data from and, if supported by the specific system, writing changes to user accounts. The connection to a target system can be managed via a direct connector or a flat file.

"**Term**" means that period(s) specified in an Order during which Customer will have access to and use of the SaaS Service.

"**User**" means an employee or independent contractor of Customer or other Identity Cube user that Customer authorises to use the SaaS Service on Customer's behalf.

2. SAAS SERVICE

2.1. Provision of SaaS Service. During the Term, SailPoint grants Customer a limited, non-exclusive, non-transferrable (except in accordance with Section 12.1 (Assignment)), non-sublicensable, royalty-free right to access and use the SaaS Service in accordance with the Documentation, solely for Customer's internal business operations, in each case subject to the terms of this SaaS Agreement, including the number of Identity Cubes and Sources documented in the Order. Customer agrees that its purchase of the Services is neither contingent upon the delivery of any future functionality or features nor dependent upon any oral or written public comments made by SailPoint with respect to future functionality or features.

2.2. Required Software. Customer acknowledges that use of the SaaS Service requires the installation of the Required Software as a pre-requisite for using the SaaS Service. Customer agrees to install such Required Software, including any required updates if and when available. SailPoint hereby grants to Customer a limited, non-exclusive, non-transferable (except in accordance with Section 12.1 (Assignment)), non-sublicensable, royalty-free license to install, execute, copy, display, or otherwise use the Required Software in accordance with the Documentation, solely in connection with the Services, during the Term, in each case subject to the terms of this SaaS Agreement.

2.3. Users. Users will be required to abide by the terms of this SaaS Agreement. Any breach by a User will be deemed to be a breach by Customer. SailPoint may terminate or suspend any User's access to the SaaS Service for any breach without notice.

2.4. SaaS Support. During the Term, SailPoint will provide Customer with support services (the "**SaaS Support**") in accordance with SailPoint's current Premium SaaS Support Policy attached hereto as Exhibit B.

2.5. Service Level Agreement. The SaaS Service Level Agreement ("**SLA**") for the production instance of the SaaS Service is set forth in SailPoint's current SLA attached hereto as Exhibit C.

3. CUSTOMER RESPONSIBILITIES AND RESTRICTIONS

3.1. Customer Responsibilities. Customer is responsible for all activities conducted by it or through the accounts of its Users on the SaaS Service. Except for SailPoint's obligations described in Section 10 (Confidentiality) and Section 11 (Data Security and Processing), Customer shall (i) have sole responsibility for the accuracy, quality, and legality of the Customer Data and the means by which Customer acquired the Customer Data and the right to provide the Customer Data for the purposes of this SaaS Agreement (including ensuring the receipt of all permissions from individuals and other third parties as may be necessary in order to provide the Customer Data for the purposes contemplated in this SaaS Agreement); (ii) be responsible for the security and confidentiality of Customer's and its Users' account information; (iii) be responsible for maintaining a back-up of all Customer Data; and (iv) prevent unauthorised access to, or use of, the Services, and notify SailPoint promptly of any such unauthorised access or use.

3.2. Compliance with Laws. Customer shall comply with all applicable local, state, national, and foreign laws, rules, and regulations ("**laws**") in connection with its use of the Services, collection and other processing of all Customer Data, and performance under this SaaS Agreement, including those laws related to employment, data privacy and protection, and international activities. Customer acknowledges that SailPoint exercises no control over the Customer Data transmitted by Customer or Users to or through the SaaS Service.

SailPoint may impose limits on the use or access to the Services as required by applicable law.

3.3. Restrictions. Customer and its Users shall not, and shall not permit any third party to: (i) copy or republish the Services; (ii) make the Services available to any person other than Users; (iii) rent, lend, sell, sublicense, or use the Services to provide service bureau, time-sharing or other services to third parties; (iv) send or store in the SaaS Service any personal health data, credit card data, personal finance data, Sensitive Personal Data (as defined in the DPA), government issued identification numbers, or other sensitive data which may be subject to regulation; (v) send or store viruses, spyware, ransomware, timebombs, Trojan horses, or other harmful or malicious code, or files to or in connection with the Services; (vi) send or store infringing, offensive, harassing or otherwise unlawful material in connection with the Services; (vii) modify or create derivative works based upon the Services or Documentation; (viii) remove, modify, or obscure any copyright, trademark, or other proprietary notices contained in the Services or Documentation; (ix) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code used or embodied in the SaaS Service, which for the avoidance of doubt includes the related algorithms, methods, and techniques; (x) access or use the Services or Documentation in order to build a similar or competitive product, or (xi) exploit the Services or Documentation in any unauthorised way whatsoever, including by trespassing or burdening network capacity. If for some reason these restrictions are prohibited by applicable law or by an agreement SailPoint has with one of its licensors, then the activities are permitted only to the extent required to comply with such law or agreement.

4. INTELLECTUAL PROPERTY

4.1. Ownership and Reservation of Rights of SailPoint Intellectual Property. SailPoint and its licensors own and, except for the limited rights expressly granted to Customer under this SaaS Agreement, retain all right, title, and interest in and to the Services, Documentation and any other materials provided by SailPoint or its licensors under this SaaS Agreement, including all modifications, derivative works, and feedback related thereto and intellectual property rights therein. No rights are granted to Customer under this SaaS Agreement other than expressly set forth in this SaaS Agreement.

4.2. Rights in Customer Data. As between SailPoint and Customer, Customer owns the Customer Data. Customer hereby grants and agrees to grant to SailPoint and its affiliates a limited-term, worldwide, non-exclusive, transferable, sublicensable, royalty-free license to host, copy, transmit, display, and process the Customer Data as reasonably necessary to provide the Services to Customer and as necessary to monitor, modify, and improve (including develop) SailPoint's services.

4.3. Feedback. To the extent Customer or any of its Users provides any suggestions for modification or improvement or other comments, code, information, know-how, or other feedback (whether in oral or written form) relating to the Services ("**Feedback**"), Customer hereby grants to SailPoint a perpetual, irrevocable, worldwide, non-exclusive, transferable, sublicensable, royalty-free license to use and commercially exploit the Feedback in any manner SailPoint sees fit without accounting or other obligation.

4.4. Statistical Usage Data. SailPoint owns the statistical usage data derived from the operation of the SaaS Service, including data regarding applications utilised in connection with the SaaS Service, configurations, log data, and the performance results for the SaaS Service ("**Usage Data**"). Nothing herein shall be construed as prohibiting SailPoint from utilising the Usage Data to monitor and improve the SaaS Service or otherwise operate SailPoint's business; provided that if SailPoint provides Usage Data to third parties, such Usage Data shall be de-identified and presented in the aggregate so that it will not disclose the identity of Customer or any human User to any third party.

5. ORDERS AND PAYMENT

5.1. Orders. Customer may purchase Services by either (a) entering into an Order with SailPoint or (b) entering into an Order with a Partner that is subsequently acknowledged by SailPoint in writing or following notification of an Order to SailPoint from the Partner, SailPoint sends a delivery notice to Customer via email. Each Order with SailPoint shall be signed by both Customer and SailPoint or issued by SailPoint and acknowledged by Customer via the issuance of a purchase order that incorporates by reference the applicable Order and subsequently accepted by SailPoint. All Orders placed through a Partner will be subject to pricing mutually agreed to between Customer and Partner. All Services purchased by Customer through either SailPoint or a Partner shall be governed exclusively by this SaaS Agreement and, subject to Section 12.5, the applicable Order.

5.2. Fees; Invoicing and Payment.

(a) Direct Purchases from SailPoint. For direct purchases with SailPoint, all fees for the Services shall be set forth in the applicable Order. All fees are exclusive of sales and use taxes, value added taxes (VAT), or similar charges. Unless otherwise provided in the Order, SailPoint shall invoice Customer for all fees described therein on the Order effective date. Customer shall pay all invoices (except with respect to charges then under reasonable and good faith dispute) net thirty (30) days from date of invoice. Except as expressly provided otherwise herein, fees are non-refundable, non-cancellable and not subject to set-off. All fees shall be stated in and paid by the Customer in the currency stated in each Order. If any fees (except with respect to charges then under reasonable and good faith dispute) remain unpaid by their due date, in addition to any other rights or remedies it may have under this SaaS Agreement or by matter of law, (i) SailPoint reserves the right to suspend the Services upon thirty (30) days written notice, until such amounts are paid in full, and (ii) any such unpaid fees may accrue, at SailPoint's discretion, late charges at the rate of the lesser of one and one-half (1.5%) percent of the outstanding balance per month or the maximum rate permitted by law from the date such fees were due until the date paid. Further, Customer shall be responsible for all costs and expenses associated with collecting such fees, including reasonable attorneys' fees. Suspension of the Services under this section shall not release Customer of its payment obligations under this SaaS Agreement.

(b) Purchases Through a Partner. For any Services purchased by Customer through a Partner, the pricing and payment terms are established by and between Customer and such Partner ("**Partner Agreement**") and all payments will be made directly to Partner. If a Partner is entitled to terminate or suspend any Services purchased by Customer through such Partner pursuant to the Partner Agreement and notifies SailPoint of such, SailPoint may suspend or terminate the Services identified by such Partner. Subsequently, if Partner notifies SailPoint that Customer is entitled to reinstatement of any Services purchased by Customer through such Partner pursuant to the Partner Agreement, and Customer is otherwise in compliance with the terms of this SaaS Agreement, SailPoint shall reinstate such Services as soon as reasonably practicable. SailPoint shall not be liable to Customer or to any third party for any liabilities, claims, or expenses arising from or relating to any suspension or termination of Services in accordance with this Section 5.2(b).

5.3. Expenses. Unless otherwise specified in an Order, Customer will reimburse SailPoint for all pre-approved, out-of-pocket travel and related expenses incurred in performing the Other Services. SailPoint will include reasonably detailed documentation of all such expenses with each related invoice.

5.4. Taxes. Customer is responsible for payment of all sales and use taxes, value added taxes (VAT), or similar charges relating to Customer's purchase and use of the Services, excluding taxes based on SailPoint's net income. If SailPoint has a legal obligation to pay or collect taxes for which Customer is responsible under this SaaS Agreement, the appropriate amount shall be computed based on Customer's address listed under Customer Information above and invoiced to and paid by Customer, which amounts are in addition to the fees for the Services, unless Customer provides SailPoint with a valid tax exemption certificate authorised by the appropriate taxing authority.

6. TERM, SUSPENSION, AND TERMINATION

6.1. Term. The term of this SaaS Agreement shall begin on the date that Customer enters into an Order pursuant to Section 5.1 (Orders) (the "**Effective Date**") and continues until the stated Term in all Orders has expired or has otherwise been terminated. This SaaS Agreement may be terminated at any time by mutual agreement of SailPoint and Customer.

6.2. Termination for Material Breach. Either party may terminate this SaaS Agreement if the other party fails to cure any material breach within thirty (30) days after receipt of written notice of such breach. Upon any termination of this SaaS Agreement by Customer for a material breach by SailPoint pursuant to this Section 6.2, SailPoint will refund Customer a pro-rata portion of any prepaid fees paid by Customer to SailPoint that cover the remainder of the Term after the effective date of termination and a pro-rata portion of any prepaid fees paid by Customer to SailPoint for Other Services that cover Other Services that have not been delivered as of the effective date of termination.

6.3. Suspension for Ongoing Harm. SailPoint reserves the right to suspend delivery of the SaaS Service if SailPoint reasonably concludes that Customer or a User's use of the SaaS Service is causing immediate and ongoing harm to SailPoint or the security, integrity, or availability of the SaaS Service. SailPoint will use commercially reasonable efforts under the circumstances to provide Customer with notice and an opportunity to remedy such violation or threat prior to such suspension. In the extraordinary case that SailPoint must suspend delivery of the SaaS Service, SailPoint shall promptly notify Customer of the suspension and the parties shall diligently attempt to resolve the issue. SailPoint shall not be liable to Customer or to any third party for any liabilities, claims or expenses arising from or relating to any suspension of the SaaS Service in accordance with this Section 6.3. Nothing in this Section 6.3 will limit SailPoint's other rights under this Section 6.

6.4. Retrieval of Customer Content. Upon request by Customer made at least thirty (30) days prior to the effective date of the termination of this SaaS Agreement, SailPoint will make available to Customer, at no cost, for a maximum of thirty (30) days following such termination for download a file of the Customer Data then-currently stored in the SaaS Service ("**Customer Content**"). After such thirty (30)-day period, SailPoint shall have no obligation to maintain or provide any Customer Content and shall thereafter, unless legally prohibited, be entitled to delete all Customer Content; provided, however, that SailPoint will not be required to remove copies of the Customer Content from its backups until such time as the backup copies are scheduled to be deleted in the normal course of business; provided further that in all cases SailPoint will continue to protect the Customer Content in accordance with Section 10 (Confidentiality). Additionally, during the Term, Customer may extract Customer Content from the SaaS Service using SailPoint's standard web services.

6.5. Effect of Termination. Upon expiration or termination of this SaaS Agreement, all licenses to the Required Software and access to the SaaS Service granted to Customer under this SaaS Agreement and all Orders placed hereunder shall immediately terminate and Customer will cease using the SaaS Service, (except as permitted under Section 6.4 (Retrieval of Customer Content)) and SailPoint Confidential Information. Expiration or termination of this SaaS Agreement for any reason other than termination by Customer for a material breach by SailPoint pursuant to Section 6.2 (Termination for Material Breach) shall not relieve Customer of the obligation to pay all future amounts due under all Orders. Sections 3.3 (Restrictions), 4 (Intellectual Property), 5.2 (Fees; Invoicing and Payment), 6.5 (Effect of Termination), 7.2 (Disclaimer), 8 (Limitations of Liability), 9 (Indemnification), 10 (Confidentiality), and 12 (General Provisions) shall survive the expiration or termination of this SaaS Agreement for any reason.

7. WARRANTIES AND REMEDIES, AND DISCLAIMERS

7.1. Warranties and Remedies.

(a) General. Each party represents and warrants that it has the legal power and authority to enter into and perform under this SaaS Agreement. SailPoint shall comply with all laws applicable to SailPoint in its performance hereunder.

(b) SaaS Service. SailPoint warrants that during the Term the SaaS Service will perform substantially in accordance with the Documentation. As Customer's exclusive remedy and SailPoint's sole liability for breach of the warranty set forth in this Section 7.1(b), (i) SailPoint shall correct the non-conforming SaaS Service at no additional charge to Customer, or (ii) in the event SailPoint is unable to correct such deficiencies after good-faith efforts and within a commercially reasonable timeframe, Customer shall be entitled to terminate the applicable SaaS Service and SailPoint will refund Customer a pro-rata portion of any prepaid fees attributable to the defective SaaS Service paid by Customer to SailPoint from the date SailPoint received the notice contemplated in the next sentence. To receive warranty remedies, Customer must promptly report deficiencies in writing to SailPoint, but no later than thirty (30) days of the first date the deficiency is identified by Customer. The warranty set forth in this Section 7.1(b) shall apply only if the applicable SaaS Service has been utilised in accordance with the Documentation, this SaaS Agreement, and applicable law.

(c) Other Services. SailPoint warrants that the Other Services will be performed in a professional manner consistent with applicable industry standards. As Customer's exclusive remedy and SailPoint's sole liability for breach of the warranty set forth in this Section 7.1(c), SailPoint will, at its sole option and expense, promptly re-perform any Other Services that fail to meet this limited warranty or refund to Customer the fees paid for the non-conforming portion of the Other Services.

7.2. Disclaimer. Except as expressly provided in this Section 7 and to the maximum extent permitted by applicable law, SailPoint makes no warranties of any kind, whether express, implied, statutory, or otherwise, and specifically disclaims all warranties of fitness for a particular purpose, merchantability, accuracy of informational content, systems integration, non-infringement, non-interference with enjoyment or otherwise. SailPoint does not warrant that the SaaS Service will be error free or uninterrupted. SailPoint makes no warranty regarding any non-SailPoint application with which the SaaS Service may interoperate. The limited warranties provided in this Section 7 are the sole and exclusive warranties provided to Customer in connection with the subject matter of this SaaS Agreement.

8. LIMITATIONS OF LIABILITY

8.1. Neither Party excludes or limits its liability for:

(a) death or personal injury caused by its negligence, or that of its employees, agents or sub-contractors;

(b) any breach by them of the "Restrictions", "Indemnification" or "Confidentiality" provisions of this Agreement;

(c) a breach of its respective obligations under the DPA due to its willful misconduct, or negligence ("negligence" not including an error of judgement or mistake in good faith) or that of its employees, contractors or agents);

(d) otherwise any willful misconduct, fraud or fraudulent misrepresentation by it or its employees; or

(e) any liability that cannot be excluded or limited by virtue of the Governing Law (as per Section 12.9 below).

8.2. Subject to Sections 8.1and 8.3;

(a) in the event of a Security Incident (as defined in the DPA) by SailPoint of any personal data of Customer that SailPoint is processing under the DPA, SailPoint's total financial liability shall not exceed 200% of the total fees paid or payable by the Customer pursuant to Section 5.2 (Fees, Invoicing and Payment) under this Agreement at the time the claim arose; and

(b) for all other claims of either party for direct/other damages under this Agreement, the aggregate liability of the other party, regardless of the nature of the claim (including negligence) and irrespective of whether the same was foreseeable or otherwise, shall not exceed 125% of the total fees paid or payable by the Customer under this Agreement at the time of such claim.

8.3. Subject to Section 8.1, in no event shall either Party be liable to the other for any, indirect, special, punitive or consequential loss or damage, including (by way of example and not an exhaustive list), loss of profits, loss of business, loss of revenue, loss of or damage to goodwill, loss of savings (whether anticipated or otherwise.

9. INDEMNIFICATION

9.1. Indemnification by SailPoint. Subject to Section 9.3 (Indemnity Process), SailPoint will defend Customer from any and all claims, demands, suits, or proceedings brought against Customer by a third party alleging that the SaaS Service, as provided by SailPoint to Customer under this SaaS Agreement, infringe any patent, copyright, or trademark or misappropriate any trade secret of that third party (each, an "**Infringement Claim**"). SailPoint will indemnify Customer for all damages and costs (including reasonable attorneys' fees) finally awarded by a court of competent jurisdiction, authorised arbitral panel, or paid to a third party in accordance with a written settlement agreement signed by SailPoint, in connection with an Infringement Claim. In the event any such Infringement Claim is brought, or in SailPoint's reasonable opinion is likely to be brought, SailPoint may, at its option: (a) procure the right to permit Customer to continue use of the SaaS Service, (b) replace or modify the SaaS Service with a non-infringing alternative having substantially equivalent performance within a reasonable period of time, or (c) if the foregoing options are not reasonably practicable, terminate the applicable Order and repay to Customer any prepaid fees paid by Customer under such Order to

SailPoint with respect to any period of time following the termination date. Notwithstanding the foregoing, SailPoint shall have no liability for any Infringement Claim of any kind to the extent that it relates to (i) modification of the SaaS Service by a party other than SailPoint, (ii) use of the SaaS Service in combination with any other product, service, or device, if the infringement would have been avoided by the use of the SaaS Service without such other product, service, or device, or (iii) use of the SaaS Service other than in accordance with the Documentation and this SaaS Agreement. The indemnification obligations set forth in this Section 9.1 are Customer's exclusive remedy and SailPoint's sole liability with respect to SailPoint's infringement or misappropriation of third-party intellectual property rights of any kind.

9.2. Indemnification by Customer. Subject to Section 9.3 (Indemnity Process), Customer will defend SailPoint from any and all claims, demands, suits, or proceedings brought against SailPoint by a third party alleging a violation of a User's or third party's rights arising from or related to the Customer Data, including the Customer's provision of the Customer Data to SailPoint or SailPoint's use of the Customer Data in connection with providing the Services in accordance with this SaaS Agreement. Customer will indemnify SailPoint for all damages and costs (including reasonable attorneys' fees) finally awarded by a court of competent jurisdiction, authorised arbitral panel, or paid to a third party in accordance with a written settlement agreement signed by Customer, in connection with an such claims, demands, suits, or proceedings.

9.3. Indemnity Process. The party seeking indemnification under this Section 9 ("**Indemnitee**") must (a) promptly notify the other party ("**Indemnitor**") of the claim (provided that any failure to provide such prompt written notice will only relieve the Indemnitor of its obligations to the extent its ability to defend such claim is materially prejudiced by such failure), (b) give the Indemnitor sole control of the defense and settlement of the claim (provided that Indemnitor shall not consent to entry of any judgment or admission of any liability of the Indemnitee without the prior written approval of the Indemnitee), and (c) provide reasonable assistance, cooperation, and required information with respect to the defense and settlement of the claim, at the Indemnitor's expense. At its own expense, the Indemnitee may retain separate counsel to advise the indemnitee regarding the defense or settlement of the claim.

10. CONFIDENTIALITY

10.1. As used in this SaaS Agreement, "**Confidential Information**" means all proprietary, non-public information disclosed by a party (the "**Disclosing Party**") to the other party (the "**Receiving Party**"), directly or indirectly, which, (a) if in written, graphic, machine-readable or other tangible form, is marked as "confidential" or "proprietary," (b) if disclosed orally or by demonstration, is identified at the time of initial disclosure as confidential and is confirmed in writing to the Receiving Party to be "confidential" or "proprietary" within thirty (30) days of such disclosure, or (c) reasonably appears to be confidential or proprietary because of the circumstances of disclosure and the nature of the information itself, including the Customer Data, terms of this SaaS Agreement, each Order, the Services and Documentation, business and marketing plans, technology and technical information, product designs, and business processes of either party.

10.2. "**Confidential Information**" does not include information that:

(a) is known publicly at the time of the disclosure by the Disclosing Party or becomes known publicly after disclosure through no fault of the Receiving Party;

(b) is known to the Receiving Party at the time of disclosure by the Disclosing Party due to previous receipt from a source that wasn't bound by confidentiality obligations to the Disclosing Party at that time; or

(c) is independently developed by the Receiving Party without use of or reference to the Confidential Information as demonstrated by the written records of the Receiving Party.

10.3. The Receiving Party shall not (a) use the Confidential Information of the Disclosing Party except to exercise its rights and perform its obligations under this SaaS Agreement or (b) disclose such Confidential Information to any third party, except those of its employees, service providers, agents, and representatives who are subject to confidentiality obligations at least as stringent as the obligations set forth herein and have a "need to know" in order to carry out the purpose of this SaaS Agreement. The Receiving Party shall use at least the same degree of care it uses to protect its own confidential information of like nature, but not less than a reasonable degree of care, to protect the Confidential Information of the Disclosing Party.

10.4. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent such disclosure is required by law or order of a court or other governmental authority; provided that the Receiving Party shall use commercially reasonable efforts to promptly notify the Disclosing Party prior to such disclosure to enable the Disclosing Party to seek a protective order or otherwise prevent or restrict such disclosure.

11. DATA SECURITY AND PROCESSING

11.1. Security Program. SailPoint will maintain administrative, physical, and technical safeguards designed to protect the security and confidentiality of Customer Data, including measures designed to prevent unauthorised access, use, modification, or disclosure of Customer Personal Data. SailPoint's current SaaS Data Security Program is described in the DPA. SailPoint will operate in conformance with the physical, technical, operational, and administrative measures and protocols regarding data security for the SaaS Service as set forth in its then current Service Organization Control 2 (SOC 2) Type 2 Report (or equivalent report), received from its third-party auditors.

11.2. Data Processing Agreement. The DPA sets forth the terms and conditions under which SailPoint may receive and process Customer Personal Data from Customer. To the extent one is required, the DPA, as entered into between SailPoint and Customer, shall apply where and only to the extent that SailPoint processes Customer Personal Data on the behalf of Customer as Data Processor (as defined in the DPA) in the course of providing Services pursuant to this SaaS Agreement.

12. GENERAL PROVISIONS

12.1. Assignment. Neither party may assign this SaaS Agreement or otherwise transfer any right or obligation under this SaaS Agreement, without the prior written consent of the other party, which consent shall not be unreasonably withheld or delayed. Notwithstanding the foregoing, either party may assign this SaaS Agreement in its entirety to an acquirer of all or substantially all of the assets or equity of such party to which this SaaS Agreement relates, whether by merger, asset sale, or otherwise so long, in the event of an assignment by Customer, as all fees then due and payable to SailPoint have been paid. Any attempt by a party to assign or transfer its rights or obligations under this SaaS Agreement other than as permitted by this Section 12.1 shall be void and of no effect. Subject to the foregoing, this SaaS Agreement shall be binding upon and inure to the benefit of the parties' successors and permitted assigns. Either party may employ subcontractors in performing its duties under this SaaS Agreement, provided, however, that such party shall not be relieved of any obligation under this SaaS Agreement and subject (as applicable) to the applicable sub-processing terms of the DPA.

12.2. Notices. Except as otherwise expressly permitted in this SaaS Agreement, notices under this SaaS Agreement shall be in writing and shall be deemed to have been given (a) five (5) business days after mailing if sent by registered or certified mail, (b) when personally delivered, or (c) one (1) business day after deposit for overnight delivery with a recognised courier for U.S. deliveries (or three (3) business days for international deliveries.

12.3. Force Majeure Event. Neither party shall be liable to the other for any delay or failure to perform hereunder due to circumstances beyond such party's reasonable control, including acts of God, acts of government, computer related attacks, hacking, or acts of terror, service disruptions involving hardware, software, or power systems not within such party's possession or reasonable control (a "**Force Majeure Event**").

12.4. Equitable Relief. The parties agree that a material breach of Section 10 (Confidentiality) or Section 3.3 (Restrictions) would cause irreparable injury to the non-breaching party for which monetary damages alone would not be an adequate remedy, and therefore the non-breaching party shall be entitled to equitable relief in addition to any other remedies it may have hereunder or at law, without the requirement of posting bond or proving actual damages.

12.5. Entire Agreement. This SaaS Agreement together with the documents incorporated herein by reference contains the entire agreement of the parties with respect to the subject matter hereof and supersedes all previous oral and written communications, representation, understandings, and agreements by the parties concerning the subject matter of this SaaS Agreement. No terms, provisions or conditions contained in any purchase order, sales confirmation, or other business form that either party may use in connection with the transactions contemplated by this SaaS Agreement will have any effect on the rights or obligations of the parties under, or otherwise modify, this SaaS Agreement. If there is any conflict between the terms of this SaaS Agreement and any Order or similar ordering document with a Partner, the terms of this SaaS Agreement shall control unless SailPoint and Customer expressly agree otherwise in the applicable Order or other document signed by both parties by specific reference to this Section and the Section(s) of this SaaS Agreement that are modified. Where SailPoint is required to "click through" or otherwise accept any online terms as a condition to its provision or receipt of Services, such terms are not binding and shall not be deemed to modify this SaaS Agreement. No modification, amendment, or waiver of any provision of this SaaS Agreement will be effective unless in writing and signed by authorised representatives of both parties hereto. Any failure to enforce any provision of this SaaS Agreement shall not constitute a waiver thereof or of any other provision and a waiver of any breach of this SaaS Agreement shall not constitute a waiver of any other or subsequent breach.

12.6. Publicity. During the term of this SaaS Agreement, SailPoint may include Customer's name and logo in its customer lists, including on its website. To the extent Customer provides standard trademark usage guidelines, SailPoint shall use Customer's name and logo in accordance with such guidelines.

12.7. Export Laws. Export laws of the United States and any other relevant local export laws apply to the Services. Customer agrees that such export laws govern its use of the Services (including technical data) and any materials provided under this SaaS Agreement, and Customer agrees to comply with all such export laws. Customer agrees that no data, information, software programs, or other materials resulting from Services (or direct product thereof) will be exported, directly or indirectly, in violation of these laws.

12.8. Independent Contractors, No Third-Party Beneficiaries. The parties have the status of independent contractors, and nothing in this SaaS Agreement nor the conduct of the parties will be deemed to place the parties in any other relationship. Except as provided in this SaaS Agreement, neither party shall be responsible for the acts or omissions of the other party or the other party's personnel. Save as contained expressly herein (or in any Order), this SaaS Agreement confers no rights upon either party's employees, agents, contractors, partners or customers or any other person or entity.

12.9. Governing Law and Severability. Where the address of the Customer (as contained in any Order) is located in any of the following countries, then the laws of such country shall apply to this SaaS Agreement and such Order(s): **Austria, Belgium, Denmark, Finland, France, Germany, Netherlands, Norway, Republic of Ireland, Spain, Sweden, Switzerland**. Where such address is located in any other country, this Agreement and all Orders will be governed by and construed in accordance with the laws of **England and Wales.** The United Nations Convention on Contracts for the International Sale of Goods does not apply. If any term of this SaaS Agreement is held to be invalid or unenforceable, that term shall be reformed.

12.10. Anti-Bribery/Corruption. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from an employee or agent of the other party in connection with this SaaS Agreement. If either party learns of any violation of the foregoing restriction, such party will use reasonable efforts to promptly notify the other party.

12.11. Interpretation. For purposes of interpreting this SaaS Agreement, (a) unless the context otherwise requires, the singular includes the plural, and the plural includes the singular; (b) unless otherwise specifically stated, the words "herein," "hereof," and "hereunder" and other words of similar import refer to this SaaS Agreement as a whole and not to any particular section or paragraph; (c) the words "include" and "including" will not be construed as terms of limitation, and will therefore mean "including but not limited to" and "including without limitation"; (d) unless otherwise specifically stated, the words "writing" or "written" mean preserved or presented in retrievable or reproducible form, whether electronic (including email but excluding voice mail) or hard copy; and (e) the captions and section and paragraph headings used in this SaaS Agreement are inserted for convenience only and will not affect the meaning or interpretation of this SaaS Agreement.

12.12. Country-Specific Contract Terms. Where, pursuant to Section 12.9 above (Governing Law and Severability) this SaaS Agreement is subject to the laws of France ("**French Law**") or Germany ("**German Law**"), certain Sections of this SaaS Agreement shall be deemed to be varied in accordance with the applicable provisions of Exhibit D attached hereto. In the event of any conflict between the provisions of Exhibit D and the provisions of this SaaS Agreement, the provisions of Exhibit D shall prevail, in relation to the context thereof.

*** End of Page ***

EXHIBIT A

Customer Data Processing Addendum

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 (a) a direct or indirect ownership interest of more than 50% or (b) 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 the agreement between Customer and SailPoint for the provision of the Services to Customer.

"**CCPA**" means the California Consumer Privacy Act.

"**Customer**" means the entity set forth in the signature block above and party to the Agreement.

"**Customer Data**" has the meaning set forth in the Agreement (if any).

"**Customer Personal Information**" means any Customer Data that is Personal Information (including Sensitive Personal Information) that Customer discloses, provides or otherwise makes available to SailPoint (either directly or indirectly) under or in connection with the Agreement.

"**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Information.

"**Data Processor**" means an entity that Processes Personal Information on behalf of a Data Controller.

"**Data Protection Act 2018**" means the Act of that name, applicable in the United Kingdom.

"**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, including, but not limited to, (where applicable) European Data Protection Law and/or the CCPA.

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

"**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; and/or (iii) the Data Protection Act 2018; and/or (iv) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i) through (ii) above, including by Switzerland.

"**Model Clauses**" means the Standard Contractual Clauses for Data Processors as approved by the European Commission in the form set out in **Annex B.**

"**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.

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

"**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 but does not include any Unsuccessful Security Incident.

"**Sensitive Personal Information**" means any Customer Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

"**Services**" means the services provided by SailPoint to Customer pursuant to the Agreement, which may include: (i) support and maintenance services for its on-premise software; (ii) SaaS services; and (iii) professional services (e.g. implementation services, expert services, and training services) provided by SailPoint to Customer pursuant to the Agreement.

"**Sub-processor**" means any Data Processor engaged by SailPoint or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or SailPoint's Affiliates. Sub-processors may also include subcontractors that are specified in an applicable SOW.

"**Unsuccessful Security Incident**" means an unsuccessful attempt or activity that does not compromise the security of Customer Personal Information, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents.

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.

Scope and Applicability of this DPA

2.1 This DPA applies where and only to the extent that: (i) SailPoint Processes Customer Personal Information on the behalf of Customer as a Data Processor in the course of providing Services pursuant to the Agreement; and (ii) Customer is subject to European Data Protection Law.

2.2 Notwithstanding expiry or termination of the Agreement and subject to Section 9 (Return or Deletion of Customer Personal Information), this DPA will remain in effect until, and will automatically expire upon, deletion or return of all Customer Personal Information by SailPoint to Customer as described in this DPA.

Roles and Scope of Processing

3.1 **Role of the Parties**. For the purposes of European Data Protection Law, SailPoint shall Process Customer Personal Information only as a Data Processor acting on behalf of Customer.

3.2 **Customer Processing of Personal Information**. Customer agrees that: (i) 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) 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. If European Data Protection Law applies to the Processing of Customer Personal Information and Customer is itself a Data Processor, Customer warrants to SailPoint that Customer's instructions and actions with respect to that

Customer Personal Information, including its appointment of SailPoint as another Data Processor, have been authorised by the relevant Data Controller.

3.3 **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. The parties agree that this DPA and the Agreement set out the Customer's complete and final 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.

3.4 **Details of Data Processing.**

(a) Subject matter: The subject matter of the Processing under this DPA is the Customer Personal Information.

(b) Duration: As between SailPoint and Customer, the duration of the Processing under this DPA is until the termination of the Agreement in accordance with its terms.

(c) Purpose: The purpose of the Processing under this DPA is the provision of the Services to the Customer and the performance of SailPoint's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties in mutually executed written form.

(d) Nature of the processing: To provide identity governance solutions and other Services as described in the Agreement, SailPoint will Process Customer Personal Information upon the instruction of the Customer in accordance with the terms of the Agreement.

(e) Categories of data subjects: Customer may disclose Customer Personal Information to SailPoint, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Information relating to the following categories of data subjects:

(i) Employees, contractors, agents, advisors, freelancers of Customer (who are natural persons); and/or

(ii) If licensed under the Agreement, Customer's business partners and/or end-users authorised by Customer to use the Services.

(f) Types of Personal Information: Customer may disclose Customer Personal Information to SailPoint, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following types of Personal Information:

(i) Identification and contact data (name, address, title, contact details);

(ii) Employment details (job title, role, manager); and/or

(iii) IT information (entitlements, IP addresses, usage data, cookies data, geolocation data).

(g) Sensitive Personal Information: Unless otherwise specified in the Agreement, Customer will not provide or make available to SailPoint Sensitive Personal Information.

3.5 **Access, Use or Sell.**

(a) SailPoint will not: (i) sell any Customer Personal Information received from Customer; or (ii) retain, access, disclose or use 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, including retaining, accessing, disclosing or using the Customer Information for a commercial purpose other than providing the Services specified in the Agreement.

(b) SailPoint shall not disclose Customer Personal Information to another business, person, or third party, except for the purpose of maintaining or providing the Services specified in the Agreement, including to provide Personal Information to advisers or sub-processors as described below, or to the extent such disclosure is required by law.

Sub-processing

4.1 **Authorised Sub-processors**. Customer agrees that SailPoint may engage Sub-processors to Process Customer Personal Information on Customer's behalf. The Sub-processors currently engaged by SailPoint and authorised by Customer are detailed in this DPA or where such detail is not included, as listed on SailPoint's website at https://www.sailpoint.com/legal/sub-processors.

4.2 **Sub-processor Obligations**. SailPoint will: (i) not engage a Sub-processor unless SailPoint enters into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Personal Information to the same standard as SailPoint; and (ii) remain responsible for its compliance with the obligations of this DPA and for any failure by the Sub-processor to fulfil its data protection obligations under the applicable Data Protection Laws.

4.3 **Changes to Sub-processors**.

(a) In relation to the list of Sub-processors on SailPoint's website at https://www.sailpoint.com/legal/sub-processors, SailPoint shall notify and request Customer's approval of any: (a) new Sub-processor it intends to grant permission; or (b) existing Sub-processor it intends to withdraw permission, in either (a) and (b), to Process Customer Personal Information ("**Request**") at least thirty (30) days prior to such grant or withdrawal, as the case may be (such notice period, the "**Review Period**").

(b) Customer acknowledges and agrees that: (a) it will make every effort to provide SailPoint with its approval of SailPoint's Request within the Review Period (such approval not to be unreasonably withheld); and (b) 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) The parties agree that: (a) any non-response by the Customer during the Review Period will be taken as the Customer's approval of that Request where Customer continues to use the Services after the Review Period has lapsed; and (b) any objection by the Customer during the Review Period will result in the parties discussing such concerns in good faith with a view to achieving a mutually beneficial resolution. If SailPoint cannot provide an alternative Sub-processor, or the parties are not otherwise able to achieve a mutually beneficial resolution as provided in (b) above, Customer, as its sole and exclusive remedy, may terminate the Services which cannot be provided by SailPoint without the use of the objected-to new Sub-processor by providing written notice to SailPoint. Upon receipt of such written notice, SailPoint will provide a pro-rata refund for prepaid fees for Services not performed/delivered as of the date of termination to Customer.

Security

5.1 **Security Measures**. Taking into account the nature of the Processing, SailPoint shall implement and maintain appropriate 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 **Annex A**, as applicable to the Services ("**Security Measures**").

5.2 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by SailPoint relating to data security and making an independent determination as to whether the Services 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.

5.3 **Customer Responsibilities**. Customer agrees that, without prejudice to SailPoint's obligations under Section 5.1 (Security Measures) and Section 8.2 (Security Incident Response):

(a) Customer is responsible for its use of the Services, including making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Information, securing its account authentication credentials, protecting the security of Customer Personal Information when in transit to and from the Services, taking appropriate steps to securely encrypt and/or backup any Customer Personal Information uploaded to the Services, and 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 by 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-premise storage).

5.4 **Customer's Security Assessment.** Customer is responsible for reviewing the Security Measures and evaluating for itself whether the Services and the Security Measures and SailPoint's commitments under this Section 5 (Security) and Section 8 (Additional Security) will meet Customer's needs, including with respect to any obligations of Customer under Data Protection Laws as applicable.

Security Reports and Audits

6.1 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 **Annex A**.

6.2 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 necessary to confirm SailPoint's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

6.3 If Customer reasonably believes that the information provided pursuant to Sections 6.1 and/or 6.2 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 no more than once every 12 months and subject to SailPoint's reasonable security and confidentiality requirements and provided that the exercise of rights under this Section 6.3 would not infringe Data Protection Laws.

International Transfers

7.1 **Data Storage and Processing Facilities**. In the event that SailPoint is providing SaaS services to the Customer, any Customer Data that the Customer uploads to the SaaS services shall remain at all times at the location of the Host (as detailed in the Agreement). With respect to its general provision of the Services, SailPoint may store and Process Customer Personal Information in SailPoint's internal systems anywhere in the world where SailPoint, its Affiliates or its Sub-processors maintain data processing operations. Where SailPoint transfers and otherwise Processes Customer Personal Information outside of the EEA, the UK or Switzerland, including by any Sub-processor, SailPoint will ensure that such transfer is made in accordance with the requirements of Data Protection Laws, such as by entering into Model Clauses.

7.2 **Model Clauses**. 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 to provide an adequate level of data protection, the parties agree to enter into and comply with the Model Clauses. SailPoint agrees that it is a "data importer" and Customer is the "data exporter" under the Model Clauses (notwithstanding that the Customer may be an entity located outside of the EEA, the UK or Switzerland).

7.3 **Alternative Transfer Mechanism.** The parties agree that the data export solution identified in Section 7.2 (Model 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) strictly 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 territories to which Customer Personal Information is transferred).

Additional Security

8.1 **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).

8.2 **Security Incident Response**. Upon confirming a Security Incident, 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.

8.3 **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. 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.

Return or Deletion of Customer Personal Information

On termination or expiration of the Agreement, Customer may wish to instruct SailPoint to delete or return all Customer Personal Information (including copies) from SailPoint's systems in accordance with applicable law. 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.

Cooperation

10.1 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 any requests from data subjects in relation to their data subject rights (e.g. right to access, erasure, deletion, to opt-out of sales, and any other similar data subject requests) under Data Protection Law or applicable data protection authorities relating to the Processing of Customer Personal Information under the Agreement. In the event that any request from data subjects or applicable data protection 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 do so, and instead, after being notified by SailPoint, Customer shall 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. For the avoidance of doubt, this Section 10.1 does not seek to diminish or exclude any right of remedy to which the data subject may be entitled pursuant to Article 82 of the GDPR.

10.2 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.

10.3 Customer acknowledges that SailPoint may be required under European Data Protection Law to: (a) collect and maintain records of certain information, including the name and contact details of each Data Processor and/or Data Controller on behalf of which SailPoint is acting and, where applicable, of such Data Processor's or Data Controller's local representative and data protection officer; and (b) 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.

10.4 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.

Relationship with the Agreement

11.1 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.

11.2 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.

11.3 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 restrict or limit the rights of any data subject or of any competent supervisory authority.

11.4 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.

11.5 This DPA and the Model Clauses will terminate simultaneously and automatically with the termination or expiry of the Agreement.

Annex A – Security Measures

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.

Security Program

- 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.
- 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.
- 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.
- 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.
- 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.

Personnel Security

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

Third-Party Security

- 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.
- 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.
- 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.

Physical Security

- 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.
- 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.
- SaaS services data center security: SailPoint leverages Amazon Web Services (AWS) data centers for hosting the SaaS services. AWS follows industry best practices and complies with numerous standards. Details on AWS data center physical security are available at https://aws.amazon.com/compliance/data-center/controls/.

Solution Security

- 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).
- 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.
- 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.

Operational Security

- 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:
  - requiring unique user IDs to identify any user who accesses systems or data;

  - managing privileged access credentials in a privileged account management (PAM) system;
  - communicating passwords separately from user IDs;
  - 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
  - automatically locking out users' IDs when a number of erroneous passwords have been entered.
- 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.
- 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.
- 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.
- 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.
- 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.
- Change management: SailPoint shall maintain change management policies and procedures to plan, test, schedule, communicate, and execute changes to SailPoint's SaaS service infrastructure, systems, networks, and applications.
- 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.
- Data segregation: SailPoint shall implement logical controls, including logical separation, access controls and encryption, to segregate Customer's Personal Data from other Customer and SailPoint data in the SaaS services. SailPoint shall additionally ensure that production and non-production data and systems are separated.

Annex B- Model Clauses

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

THE PARTIES HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. **Definitions**

For the purposes of the Clauses:

'personal data', **'special categories of data'**, **'process/processing'**, **'controller'**, **'processor'**, **'data subject'** and **'supervisory authority'** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

'the data exporter' means the controller who transfers the personal data;

'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. **Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. **Third-party beneficiary clause**

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. **Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, unless the data exporter is established in the UK, in which case, English law will apply.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Subprocessing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

11.2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Data exporter*:* The data exporter is the entity identified as the "Customer" in the Data Processing Addendum in place between data exporter and data importer and to which these Clauses are appended ("**DPA**").

Data importer*:* The data importer is the US headquartered company, SailPoint Technologies, Inc. ("**SailPoint**"). SailPoint provides identity governance solutions and other Services as described in the Agreement which process Customer Personal Information upon the instruction of the Customer in accordance with the terms of the Agreement.

Description of Data Processing: Please see Section 3.4 (Details of Processing) of this DPA for a description of the data subjects, categories of data, special categories of data and processing operations.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

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

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to

suspend the transfer of data and/or terminate the contract.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").

4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 6 (Security Reports and Audits) of the DPA.

Clause 5(j): Disclosure of sub-processor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward sub-processor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to sub-processor confidentiality restrictions, data importer may be restricted from disclosing onward sub-processor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any sub-processor it appoints to permit it to disclose the sub-processor agreement to data exporter.

3. Even where data importer cannot disclose a sub-processor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such sub-processing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability to a data subject with respect to any data subject rights under these Clauses.

Clause 11: Onward sub-processing

4. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward sub-processing by the data importer.

5. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 4 (Sub-processing) of the DPA.

EXHIBIT B - Premium SaaS Support Policy

This Attachment details SailPoint's premium identity and access management support and maintenance services to the Customer's applicable SaaS Service.

1. SaaS Support Entitlement

During the SaaS subscription term identified in an Order, Customer will receive Premium SaaS Support that includes i) support_seven (7) days a week twenty-four (24) hours a day for Severity 1 problems and ii) support during business hours of Monday-Friday, 8am-6pm local time elected by Customer excluding local holidays for all other severity problems.

2. Premium SaaS Support

SaaS Support provides Customer with the following services:

a) Telephone or electronic support in order to help Customer locate and correct problems with the SaaS.

b) Bug fixes and code corrections to correct SaaS malfunctions to bring such SaaS into substantial conformity with the operating specifications.

c) All extensions, enhancements and other changes that SailPoint, at its sole discretion, makes or adds to the SaaS and which SailPoint furnishes, without charge, to all other customer of SaaS.

3. Response and Resolution Goals

- "business hours" coverage (Monday-Friday, 8am-6pm local time elected by Customer excluding local holidays)
- "Problem" means a defect in SaaS as defined in SailPoint's SaaS specification which significantly degrades such SaaS.
- "Fix" means the repair or replacement of SaaS component in the form of a patch or e-fix to remedy Problem.
- "Workaround" means a change in the procedures followed or data supplied by Customer to avoid a Problem without substantially impairing Customer's use of the SaaS.
- "Respond" means acknowledgement via email of Problem received containing assigned support engineer name, date and time assigned, severity assignment, and other information

Problem Severity	***Response Times***	***Resolution Goals***
1. The SailPoint application is completely unavailable or seriously impacted, and there is no reasonable workaround currently available.	SailPoint will Respond within 30 minutes for Severity 1 issues and within 1 business hour for all other severity issues.	Upon confirmation of receipt, SailPoint will begin continuous work on the Problem; provided that a Customer resource is available at any time to assist with Problem determination. SailPoint will use commercially reasonable efforts to provide a Workaround or Fix within 8 hours, once the Problem is reproducible or once SailPoint has identified the defect. SailPoint may incorporate a Fix for the Problem in a future release of the SaaS service.
2. The system or SailPoint application is seriously affected. The issue is not critical and does not comply with the Severity 1 conditions. There is no workaround currently available or the workaround is cumbersome to use.	SailPoint will Respond within 1 business hour.	SailPoint will provide commercially reasonable efforts to provide a Workaround or Fix within 3 business days.
3. The system or SailPoint application is moderately affected. The issue is not critical and the system has not failed. The issue has been identified and does not hinder normal operation, or the situation may be temporarily circumvented using an available workaround.	SailPoint will Respond within 1 business hour.	SailPoint will provide commercially reasonable efforts to provide a Workaround or Fix within 7 business days.
4. Non-critical issues, general questions, or situations where functionality does not appear to match documented specifications but has no business impact.	SailPoint will Respond within 1 business hour.	SailPoint will provide commercially reasonable efforts to provide an answer within 10 business days. Resolution of a problem may appear in a future release of the SaaS.

4. Accessing Support

In addition to online help in the SaaS, which can be accessed by clicking the "Help" tab when logged into the SaaS service, function-specific help information can also be accessed throughout the SaaS using the '?' option.

The Compass online community (https://community.sailpoint.com) is available 24x7 for self-service technical assistance including:

- Accessing our knowledgebase, product documentation, technical articles, and FAQs
- Viewing supported platforms and hardware

The online support portal (http://www.sailpoint.com/services/online-support) is used to manage Customer cases and includes:

- Logging support cases and case communication
- Submitting new product enhancements
- Support Policy documentation
- Reporting status of cases

The support email address is support@sailpoint.com. Local and toll-free support phone numbers are listed in SailPoint's Compass online community.

Access to Support is available to a maximum of 10 named contacts per contract, list to be provided and maintained by Customer.

EXHIBIT C – Service Level Agreement

This Attachment details SailPoint's Service Level Agreement ("**SLA**") for the Customer's production instance of the SaaS Service.

1. Standard Terms.

   a. During each calendar month of the Term, SailPoint warrants at least 99.9% System Availability.

   b. System Availability is calculated per calendar month by:

      i. Dividing (x) the total minutes during which the user interface of the SaaS Service in a Customer production instance are available in the month *minus* the total minutes of scheduled maintenance in the month, by (y) the total minutes in the month *minus* the total minutes of scheduled maintenance in the month; and

      ii. Multiplying such result by 100.

      For purposes of calculating System Availability, only SaaS Service unavailability exceeding 30 seconds will apply.

   c. SailPoint reserves the right to take the SaaS Service offline for scheduled maintenance for which Customer has been provided reasonable notice and SailPoint reserves the right to change its maintenance window upon prior notice to Customer.

2. Exclusions. Customer shall not have any remedies under this SLA to the extent any SLA Claim is due to unavailability of the SaaS Service resulting from: (a) a Force Majeure Event, (b) issues associated with the Customer's computing devices, local area networks, or internet service provider connections, (c) use of the SaaS Service outside the scope described in this SaaS Agreement, or (d) inability to deliver the SaaS Service due to acts or omissions of Customer or any User.

3. SLA Claims. Customer must notify SailPoint customer service via support ticket within five (5) business days from the occurrence of the SLA incident and provide the details of the incident (a "**SLA Claim**"). SailPoint will use log files, database records, audit logs and any other information available to validate an SLA Claim and make a good faith judgment on the applicability of this SLA to such SLA Claim. In the event an SLA Claim is denied, SailPoint shall make the information used to validate such SLA Claim available for auditing by Customer at Customer's request.

4. Service Credits. If System Availability is less than 99.9% in an individual month and if Customer has fulfilled all of its obligations under the SaaS Agreement, then upon Customer submitting and SailPoint validating an SLA Claim, SailPoint will issue a Service Credit in Customer's next invoice, calculated in accordance with the below chart. "Service Credit" represents a percentage of the monthly fee associated with the affected SaaS Service. In any given calendar month, Customer shall in no event be entitled to receive a Service Credit that exceeds 50% of its monthly fee for the affected SaaS Service.

% System Availability	Service Credit
< 99.9%	10%
< 99.0%	20%
< 98.0%	30%
< 97.0%	40%
< 96.0%	50%

5. Alternative Remedies.

   a. At Customer's election through written request, in lieu of the foregoing Service Credit, SailPoint shall provide a credit to Customer in the equivalent dollar amount as the Service Credit to be used for additional Identity Cubes, a Term extension, or future SaaS Service renewals.

   b. If SailPoint fails to meet its obligations under the terms of this SLA for (i) three (3) consecutive months or (ii) five (5) months during a calendar year period, then Customer may, in its sole discretion, terminate the SaaS Agreement without penalty and SailPoint shall immediately refund to Customer a pro-rata portion of any prepaid fees paid by Customer to SailPoint that cover the remainder of the Term after the effective date of termination. If Customer desires to terminate the SaaS Agreement pursuant to this provision, Customer must provide written notice to SailPoint pursuant to the SaaS Agreement of such election within ten (10) calendar days of the last day of the three (3) consecutive month period in section (i) of the preceding sentence or the fifth (5th) month in section (ii) of the preceding sentence.

   c. The remedies stated in this SLA are Customer's sole remedies and SailPoint's exclusive liability for interruption of SaaS Service and SailPoint's failure to meet System Availability.

6. Miscellaneous. Customer may inquire at any time as to SailPoint's compliance with the provisions of this SLA by way of accessing SailPoint's general status website, located currently at http://status.sailpoint.com.

EXHIBIT D – Country-Specific Contract Terms

1. Where French Law applies:

(a) The parties to this Agreement do not intend to condition their engagement to a period of reflection, as mentioned in Article 1122 of the French Civil Code.

(b). The parties, fully informed of their rights under Article 1195 of the Civil Code, expressly exclude the application to unforeseen circumstances, as defined in Article 1195 of the Civil Code, regardless of the circumstances beyond the parties' control. The parties agree to assume the risks relating to any change in circumstances unforeseeable as of the Effective Date that would render its performance excessively onerous for a party, and expressly waive the right to request any renegotiation and/or judicial and/or non-judicial review of this Agreement on the hardship basis.

(c). By way of derogation from the provisions of article 1221 and article 1222 of the Civil Code, the parties agree in the event SailPoint fails to fulfill its obligations, Customer may not request forced execution and/or enforce SailPoint's obligation by itself or by a third party, at the expense of SailPoint. If such event occurs, Customer shall send a prior written notice to SailPoint related to the non-performance and the provisions as agreed in Section 6.6 of this SaaS Agreement, shall apply only.

(d). By way of derogation from the provisions of article 1223 of the Civil Code, the parties agree in the event SailPoint fails to fulfill its obligations, Customer may not reduce the price proportionally.

(e). The notice to perform SailPoint's obligations will take effect only if it refers expressly to the non-performance and Section 6.2. of this Agreement.

(f). In relation to Section 5.2 (Fees, Invoicing and Payments) of this Agreement:

- i. It is expressly agreed between the parties that in relation to a notice pursuant to such Section 5.2, Customer will be validly put on formal notice of Customer to comply with its payment obligations, in accordance with the provisions of article 1344 of the Civil Code.
- ii. No discount will be granted in the event of early payment.
- iii. Customer delaying any payment properly due and owing to SailPoint becomes a debtor to SailPoint automatically, in addition to the penalties for late payment, of a fixed allowance for recovery costs of forty (40) euros according to articles L441-10 and D441-5 of the French commercial code. SailPoint reserves the right to claim an additional compensation justifying having spent more than forty (40) euros for recovery costs.

2. Where German law applies:

(a) Limitation of Liability. Section 8 of this SaaS Agreement (Limitation of Liability) shall be replaced in its entirety with the following provisions:

(i) Neither Party excludes or limits its liability;

1. in case of intent and gross negligence;

2. in case of injury of body, life or health;

3. for any breach of the "Indemnification" or "Confidentiality" provisions of this SaaS Agreement;

4. for a breach of its respective obligations under the DPA due to willful misconduct, or gross negligence;

5. in case of a warranty (Garantie), for losses arising from the lack of any warranted characteristics, up to the amount of damage which, given the purpose of the warranty, could be typically expected and which was foreseeable for SailPoint at the time the warranty was given;

6. according to the German Product Liability Act (Produkthaftungsgesetz) in the event of product liability.

(ii) In case of breach of any material duty, which was essential for the conclusion of this SaaS Agreement an on the Performance on which the other party may rely (Kardinalspflicht), through simple negligence, the liability of the infringing party shall be limited to the amount which was foreseeable and typical with regard to the time and kind of the respective action.

(iii) SailPoint shall be liable for loss of data only up to the amount of typical recovery costs which would have arisen had proper and regular data backup measures been taken by the Customer;

(iv) A further liability does not subsist. The preceding limitation of liability does also apply with regard to personal liability of each party's employees, representatives and board members.

(v) *Both parties hereunder specifically acknowledge that the limitations of liability and exclusion of damages stated herein are reflected in the pricing and, but for such limitations and exclusions, SailPoint would not have provided the services to Customer*.

(b) Warranties. In deviation from Section 7.2 of this SaaS Agreement (Disclaimer), the language "*SailPoint does not warrant that the SaaS service will be error free or uninterrupted"* shall be deemed to be deleted and apart from the warranties explicitly mentioned in Section 7.1 (Warranties and Remedies), nothing in this SaaS Agreement shall be construed as a warranty.

(c) Other amendments.

(i) In deviation from Section 5.2(a) (Direct Purchases from SailPoint), late charges shall always accrue at the statutory default interest rate of 9 percentage points above the basic rate of interest per year (Sec. 288 para 2 German Civil Code).

(ii) In addition to Section 6.2 (Termination for Material Breach), SailPoint shall also reimburse the Customer for all fees already paid for Services which were provided before the termination came into effect, insofar as the Customer proves that the Services had no value to him up to this point in time due to the circumstance which led to the termination.