SOFTWARE AS A SERVICE AGREEMENT (EMEA) (v10-11-20)

PLEASE READ THIS AGREEMENT BEFORE USING SAILPOINT'S SERVICES. BY ACCESSING OR USING SAILPOINT'S IDENTITY MANAGEMENT SOFTWARE AS A SERVICE OFFERING ("SaaS"), YOU ("the Customer") SIGNIFY ACCEPTANCE OF AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT ACCESS OR USE THE SaaS 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 AGREEMENT.

This Software as a Service Agreement ("**SaaS Agreement**") is entered into between Customer and SailPoint Technologies, Inc., a Delaware corporation ("**SailPoint**"), with its principal place of business at 11120 Four Points Dr., Suite 100, Austin, Texas 78726, USA. SailPoint and the Customer agree that the following terms and conditions will apply to the services provided under this Agreement and any Orders placed thereunder.

IN CONSIDERATION of the terms and conditions contained herein, it is hereby agreed by the parties as follows:

1. DEFINITIONS

"**Administrator User**" means each Customer employee designated by Customer to serve as technical administrator of the SaaS Services on Customer's behalf. Each Administrator User must complete training and qualification requirements reasonably required by SailPoint.

"Anti-Corruption Laws" shall mean all local and international laws and regulations concerning fraud, bribery and corruption, including but not limited to (and as applicable) the UK Bribery Act of 2010 and the United States Foreign Corrupt Practices Act 1977.

"Data Protection Addendum" or "DPA" means the provisions detailed in Schedule D hereto.

"Data Protection Laws" means in relation to any personal data (if any) which is processed in the performance of this SaaS Agreement, the laws as outlined in the Exhibit D, Data Processing Agreement.

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

"**Host**" means the computer equipment on which the Software is installed, which is owned and operated by SailPoint or its subcontractors.

"Identity Cube" means a unique collection of identity data for an individual that will be granted access to and/or managed by the SaaS Services for the purposes of managing passwords or certifying user access. Identity data may be physically or logically maintained in a single repository or in separate physical or logical repositories. Although Identity Cubes for user accounts that have been deactivated may remain in the identity management system, those inactive Identity Cubes will not be included in the number of Identity Cube licenses in use by Customer.

"Order" means the document(s) by which Customer orders SaaS Services and/or Other Services pursuant to this Agreement. An Order may consist of either (a) a schedule, quotation, or statement of work that has been signed by both Customer and SailPoint, and/or (b) if applicable, a purchase order issued by Customer pursuant to this Agreement that incorporates by reference the applicable Order. Orders placed with a Customer purchase order only and all orders placed through a Partner shall be governed solely by the terms of this Agreement and those of the incorporated and referenced Order.

"**Other Services**" means all technical and non-technical services performed or delivered by SailPoint under this SaaS Agreement, including, without limitation, implementation services and other professional services, training and education services but excluding the SaaS Services and the Support and Maintenance Services. Other Services will be provided on a time and material basis at such times or during such periods, as may be specified in an Order and mutually agreed to by the parties. The scope of Other Services will include, but not be limited to, implementation support, best practices consultations, integration efforts and informal training. All Other Services will be provided on a non-work for hire basis.

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

"**SaaS Services**" refer to the specific SailPoint internet-accessible service(s) identified in an Order that provides use of SailPoint's identity/access management Software that is hosted by SailPoint or its service provider and made available to Customer over a network on a term-use basis.

"Schedule" is a written document attached to this SaaS Agreement under Exhibit A or similar document executed separately by SailPoint and Customer for the purpose of purchasing SaaS Services under the terms and conditions of this SaaS Agreement.

"**Software**" means the object code version of any software to which Customer is provided access as part of the Service, including any updates or new versions.

"**Subscription Term**" or "SaaS Term" shall mean that period specified in an Order during which Customer will have on-line access and use of the Software through SailPoint's SaaS Services. At the end of the initial Subscription Term the SaaS Services subscription can be renewed for up to two additional one year terms. The per user subscription fee for SaaS Services of the same type and quantity purchased under this SaaS Agreement may be increased by no more than six percent per annum for each of the optional one-year renewal periods. In order to extend the Subscription Term both parties will mutually agree to and execute a follow-on Order.

"**Support and Maintenance Services**" means the support and maintenance services provided by SailPoint to Customer pursuant to this SaaS Agreement and Exhibit B.

2. SAAS SERVICES

2.1 During the Subscription Term, Customer will receive a nonexclusive, non-assignable, royalty free, worldwide right to access and use the SaaS Services solely for Customer's internal business operations, subject to the terms of this SaaS Agreement and up to the number of Identity Cubes documented in the Order.

2.2 Customer acknowledges that this SaaS Agreement is a services agreement and SailPoint will not be delivering copies of the Software to Customer as part of the SaaS Services.

3. RESTRICTIONS

Customer shall not, and shall not permit anyone to:

(i) copy or republish the SaaS Services or Software,

(ii) make the SaaS Services available to any person other than authorised Identity Cube users,

(iii) use or access the SaaS Services to provide service bureau, time-sharing or other computer hosting services to third parties,

(iv) modify or create derivative works based upon the SaaS Services or Documentation,

(v) remove, modify or obscure any copyright, trademark or other proprietary notices contained in the software used to provide the SaaS Services or in the Documentation,

(vi) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of the Software used to provide the SaaS Services, except and only to the extent such activity is expressly permitted by applicable law, or

(vii) access the SaaS Services or use the Documentation in order to build a similar product or competitive product. Subject to the limited licenses granted herein, SailPoint shall own all right, title and interest in and to the Software, services, Documentation, and other deliverables provided under this SaaS Agreement, including all modifications, improvements, upgrades, derivative works and feedback related thereto and intellectual property rights therein. Customer agrees to assign all right, title and interest it may have in the foregoing to SailPoint.

4. CUSTOMER RESPONSIBILITIES

4.1 Assistance. Customer shall provide commercially reasonable information and assistance to SailPoint to enable SailPoint to deliver the SaaS Services. Customer acknowledges that SailPoint's ability to deliver the SaaS Services in the manner provided in this SaaS Agreement may depend upon the accuracy and timeliness of such information and assistance.

4.2 Compliance with Laws. Customer shall comply with all applicable local, state, national and foreign laws in connection with its use of the SaaS Services, including those laws related to data privacy, international

communications, and the transmission of technical or personal data. Customer acknowledges that SailPoint exercises no control over the content of the information transmitted by Customer or the Identity Cube users through the SaaS Services. Customer shall not upload, post, reproduce or distribute any information, software or other material protected by copyright, privacy rights, or any other intellectual property right without first obtaining the permission of the owner of such rights.

4.3 Unauthorised Use; False Information. Customer shall: (a) notify SailPoint immediately of any unauthorised use of any password or user id or any other known or suspected breach of security, (b) report to SailPoint immediately and use reasonable efforts to stop any unauthorised use of the SaaS Services that is known or suspected by Customer or any Identity Cube user, and (c) not provide false identity information to gain access to or use the SaaS Services.

4.4 Administrator Access. Customer shall be solely responsible for the acts and omissions of its Administrator Users. SailPoint shall not be liable for any loss of data or functionality caused directly or indirectly by the Administrator Users.

4.5 Customer Input. Customer is solely responsible for collecting, inputting and updating all Customer information stored on the Host ("Customer Content") and for ensuring (a) that the Customer Content does not include anything that actually or potentially infringes or misappropriates the copyright, trade secret, trademark or other intellectual property right of any third party or contain anything that is obscene, defamatory, harassing, offensive or malicious, and (b) that Customer has collected and handled all Customer Content in compliance with all applicable data privacy and protection laws, rules, and regulations.

4.6 License from Customer. Subject to the terms and conditions of this SaaS Agreement, Customer shall grant to SailPoint a limited, non-exclusive and non-transferable license, to copy, store, configure, perform, display and transmit Customer Content solely as necessary to provide the SaaS Services to Customer.

4.7 Ownership and Restrictions. Customer retains ownership and intellectual property rights in and to its Customer Content. SailPoint or its licensors retain all ownership and intellectual property rights to the services, Software programs, and anything developed and delivered under the SaaS Agreement.

4.8 Suggestions. SailPoint shall have a royalty-free, worldwide, irrevocable, perpetual license to use and incorporate into the SaaS Services any suggestions, enhancement requests, recommendations or other feedback provided by Customer, including Users, relating to the operation of the SaaS Services.

5. ORDERS AND PAYMENT

5.1 Orders. Customer may purchase SaaS Services directly with SailPoint by executing an Order, or through a Partner, pursuant to an ordering document agreed to by Customer and Partner. All SaaS Services or Other Services purchased by Customer through either SailPoint or a Partner shall be governed exclusively by this SaaS Agreement and the applicable Order.

5.2 Invoicing and Payment.

(a) Direct Deals with SailPoint. Unless otherwise provided in the Order, SailPoint shall invoice Customer for all fees on the Order effective date. Customer shall pay all undisputed invoices within 30 days after Customer receives the invoice. Except as expressly provided otherwise, fees are non-refundable. All fees shall be stated in and paid by the Customer in the currency contained in each Order.

(b) Resell Deals Sold through Partner. For any SaaS Services or Other Services purchased by a Customer through a Partner, the pricing and payment terms are established between Customer and the Partner and all payments will be made directly to the Partner.

5.3 Expenses. Customer will reimburse SailPoint for its reasonable, out-of-pocket travel and related expenses incurred in performing the Other Services. SailPoint shall notify Customer prior to incurring any such expense. SailPoint shall comply with Customer's travel and expense policy if made available to SailPoint prior to the required travel.

5.4 Taxes. SailPoint shall bill Customer for applicable taxes as a separate line item on each invoice. Customer shall be 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. Customer shall not be liable for taxes based on SailPoint's net income, capital or corporate franchise.

6. TERM AND TERMINATION

6.1 Term of SaaS Agreement. The term of this SaaS Agreement shall begin on the Effective Date and shall continue until terminated by either party as outlined in this Section.

6.2 Termination. Either party may terminate this SaaS Agreement immediately upon a material breach by the other party that has not been cured within thirty (30) days after receipt of written notice of such breach.

6.3 Suspension for Non-Payment. SailPoint reserves the right to suspend delivery of the SaaS Services if Customer fails to timely pay any undisputed amounts due to SailPoint under this SaaS Agreement, but only after SailPoint notifies Customer of such failure and such failure continues for thirty (30) days or more after the payment due date. Suspension of the SaaS Services shall not release Customer of its payment obligations under this SaaS Agreement. Customer agrees that SailPoint shall not be liable to Customer or to any third party for any liabilities, claims or expenses arising from or relating to suspension of the SaaS Services resulting from Customer's nonpayment.

6.4 Suspension for Ongoing Harm. SailPoint reserves the right to suspend delivery of the SaaS Services if SailPoint reasonably concludes that Customer or an Identity Cube user's use of the SaaS Services is causing immediate and ongoing harm to SailPoint or others. In the extraordinary case that SailPoint must suspend delivery of the SaaS Services, SailPoint shall immediately 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 Services in accordance with this Section 6.4. Nothing in this Section 6.4 will limit SailPoint's rights under Section 6.5 below.

6.5 Effect of Termination.

(a) Upon termination of this SaaS Agreement or expiration of the Subscription Term, SailPoint shall immediately cease providing the SaaS Services and all usage rights granted under this SaaS Agreement shall terminate.

(b) If SailPoint terminates this SaaS Agreement due to a material, uncured breach by Customer, then Customer shall immediately pay to SailPoint or the applicable Partner (if purchased through a Partner) all amounts then due or to become due during any Order Subscription Terms issued under. If Customer terminates this SaaS Agreement due to an uncured material breach by SailPoint, then SailPoint shall immediately refund to Customer all pre-paid amounts for any unperformed SaaS Services scheduled to be delivered after the termination date.

(c) Upon termination of this SaaS Agreement and upon subsequent written request by the disclosing party, the receiving party of tangible Confidential Information shall promptly return such information or destroy such information and provide written certification of such destruction, provided that the receiving party may permit its legal counsel to retain one archival copy of such information in the event of a subsequent dispute between the parties.

7. SERVICE LEVEL AGREEMENT

The Service Level Agreement ("**SLA**") for the SaaS Services is set forth in Exhibit C hereto. The SLA sets forth Customer's sole remedies for availability or quality of the SaaS Services, including any failure to meet any guarantee set forth in the SLA.

8. WARRANTIES

8.1 Warranty. SailPoint represents and warrants that (i) SailPoint has validly entered in this SaaS Agreement and has the legal power to do so, and (ii) SailPoint will provide the SaaS Services in a professional manner consistent with general industry standards and that the SaaS Services will perform substantially in accordance with the Documentation. For any material breach of any foregoing warranty, Customer's exclusive remedy shall be as provided in Section 6, Term and Termination.

8.2 SailPoint does not guarantee that the SaaS Services will be performed error-free or uninterrupted, or that SailPoint will correct all SaaS Services errors. Customer acknowledges that SailPoint does not control the transfer of data over communications facilities, including the Internet, and that the SaaS Service may be subject to limitations, delays, and other problems inherent in the use of such communications facilities. This Section 8 sets forth the sole and exclusive warranty given by SailPoint (express or implied) with respect to the subject matter of this SaaS Agreement. Neither SailPoint nor any of its licensors or other suppliers warrant or guarantee that the operation of the SaaS Services will be uninterrupted, virus-free or error-free, nor shall SailPoint or any of its service providers be liable for unauthorised alteration, theft or destruction of Customer's or any User's data, files, or programs.

9. LIMITATIONS OF LIABILITY

9.1 Neither Party excludes or limits its liability for:

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

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

(iii) 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);

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

(v) any liability that cannot be excluded or limited by virtue of the Governing Law (pursuant to Section 14.14 below) of this Agreement.

9.2 Subject to Sections 9.1 and 9.3;

9.2.1 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 under this Agreement at the time the claim arose; and

9.2.2 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.

9.3 Subject to Section 9.1, 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).

10 INDEMNIFICATION

10.1 Indemnification by SailPoint. If a third party makes a claim against Customer that the SaaS Services infringes any patent, copyright or trademark, or misappropriates any trade secret, or that SailPoint's negligence or willful misconduct has caused bodily injury or death, SailPoint shall defend Customer and its directors, officers and employees against the claim at SailPoint's expense and SailPoint shall pay all losses, damages and expenses (including reasonable attorneys' fees) finally awarded against such parties or agreed to in a written settlement agreement signed by SailPoint, to the extent arising from the claim. SailPoint shall have no liability for any claim based on (a) the Customer Content, (b) modification of the SaaS Services not authorised by SailPoint, or (c) use of the SaaS Services other than in accordance with the Documentation and this SaaS Agreement. SailPoint may, at its sole option and expense, procure for Customer the right to continue use of the SaaS Services, modify the SaaS Services in a manner that does not materially impair the functionality, or terminate the Subscription Term and repay to Customer any amount paid by Customer with respect to the Subscription Term following the termination date.

10.2 Indemnification by Customer. If a third party makes a claim against SailPoint that the Customer Content infringes any patent, copyright or trademark, or misappropriates any trade secret, Customer shall defend SailPoint and its directors, officers and employees against the claim at Customer's expense and Customer shall pay all losses, damages and expenses (including reasonable attorneys' fees) finally awarded against such parties or agreed to in a written settlement agreement signed by Customer, to the extent arising from the claim.

10.3 Conditions for Indemnification. A party seeking indemnification under this section shall (a) promptly notify the other party of the claim, (b) give the other party sole control of the defence and settlement of the claim, and (c) provide, at the other party's expense for out-of-pocket expenses, the assistance, information and authority reasonably requested by the other party in the defence and settlement of the claim.

11 CONFIDENTIALITY

11.1 Definition. "**Confidential Information**" means any information disclosed by a party to the other 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 30 days of such

disclosure, (c) is specifically deemed to be confidential by the terms of this SaaS Agreement, or (d) reasonably appears to be confidential or proprietary because of the circumstances of disclosure and the nature of the information itself. Confidential Information will also include information disclosed by third parties to a disclosing party under an obligation of confidentiality. SailPoint Software and Documentation are deemed Confidential Information of SailPoint.

11.2 Confidentiality. During the term of this SaaS Agreement, any Confidential Information disclosed will be protected for a period of three (3) years from date of disclosure (perpetually in the case of intellectual property), each party shall treat as confidential all Confidential Information of the other party, shall not use such Confidential Information except to exercise its rights and perform its obligations under this SaaS Agreement, and shall not disclose such Confidential Information to any third party. Without limiting the foregoing, each party shall use at least the same degree of care, but not less than a reasonable degree of care, it uses to prevent the disclosure of its own confidential information to prevent the disclosure of Confidential Information of the other party. Each party shall promptly notify the other party of any actual or suspected misuse or unauthorised disclosure of the other party's Confidential Information. Neither party shall reverse engineer, disassemble or decompile any prototypes, software or other tangible objects which embody the other party's Confidential Information and which are provided to the party hereunder. Each party may disclose Confidential Information of the other party on a need-to-know basis to its contractors who are subject to confidentiality agreements requiring them to maintain such information in confidence and use it only to facilitate the performance of their services on behalf of the receiving party.

11.3 Exceptions. Confidential Information excludes information that:

(a) is known publicly at the time of the disclosure or becomes known publicly after disclosure through no fault of the receiving party,

(b) is known to the receiving party, without restriction, at the time of disclosure or becomes known to the receiving party, without restriction, from a source other than the disclosing party not bound by confidentiality obligations to the disclosing party, or

(c) is independently developed by the receiving party without use of the Confidential Information as demonstrated by the written records of the receiving party.

The receiving party may disclose Confidential Information of the other 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 reasonable efforts to promptly notify the other party prior to such disclosure to enable the disclosing party to seek a protective order or otherwise prevent or restrict such disclosure. Each party may disclose the existence of this SaaS Agreement and the relationship of the parties, but agrees that the specific terms of this SaaS Agreement will be treated as Confidential Information; provided, however, that each party may disclose the terms of this SaaS Agreement to those with a need to know and under a duty of confidentiality such as accountants, lawyers, bankers and investors.

12 INSURANCE

For the duration of this Agreement, SailPoint shall arrange and keep in effect, applicable insurance policies to cover its obligations and responsibilities hereunder (and as may be required for its business operations generally or by applicable law) and shall pay all premiums for the same at all times. SailPoint may be required at any time (but no more than annually) and upon written request of the Customer to provide documentary evidence to the Customer of the validity of the insurances, by way of written confirmation for the same as may be issued by the applicable insurer(s).The existence of such insurance policies, no matter their term or the amount insured, shall not release SailPoint in any way from its legal liability and responsibilities under the scope of this Agreement.

13 CERTIFICATIONS AND DATA PROTECTION SECURITY MEASURES

Notwithstanding the provisions contained in the DPA, it is agreed by the parties as follows:

13.1 Cross Border Transfers. Where Personal Data originates from the European Economic Area and is transferred to the United States, SailPoint will act in compliance with the EU-U.S. Privacy Shield Framework. Where Personal Data originates from Switzerland and is transferred to the United States, SailPoint will act in compliance with the U.S.-Swiss Safe Harbor Framework. SailPoint has self-certified to the EU-U.S. Privacy Shield Framework and the U.S.-Swiss Safe Harbor Framework and will maintain such certification throughout the term of this Agreement.

13.2 Audits and Certifications. SailPoint has completed a SOC 2 Type 2 audit and ISO 27001 certification. SailPoint will complete a SOC 2 Type 2 audit annually and maintain ISO 27001 certification throughout the term of this Agreement or until such time as SailPoint receives any industry certification applicable to the SaaS Services which supersedes such certifications. Upon written request from Customer, SailPoint will provide a copy of such then- current certifications and audit reports.

13.3 **Security Measures as further defined in Exhibit D, Data Processing Addendum ("DPA")**

(a) **Security Measures**. SailPoint shall implement and maintain appropriate technical and organisational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data, in accordance with SailPoint's security standards described in DPA **Annex A** ("**Security Measures**").

(b) **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 SaaS 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 SaaS Services.

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

(d) Customer is responsible for its use of the SaaS Services, including making appropriate use of the SaaS Services to ensure a level of security appropriate to the risk in respect of the Customer Data, securing its account authentication credentials, protecting the security of Customer Personal Data when in transit to and from the SaaS Services, taking appropriate steps to securely encrypt and/or backup any Customer Personal Data uploaded to the SaaS Services, and properly configuring the SaaS Services and using available features and functionalities to maintain appropriate security in light of the nature of the Customer Personal Data processed by Customer's use of the SaaS Services; and

(e) SailPoint has no obligation to protect Customer Data that Customer elects to store or transfer outside of SailPoint's and its Sub-processors' systems (for example, offline or on-premise storage).

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

14 GENERAL PROVISIONS

14.1 Non-Exclusive Service. Customer acknowledges that SaaS Services are provided on a non-exclusive basis. Nothing shall be deemed to prevent or restrict SailPoint's ability to provide the SaaS Services or other technology, including any features or functionality first developed for Customer, to other parties.

14.2 Assignment. Neither party may assign this SaaS Agreement or any right under this SaaS Agreement, without the consent of the other party, which consent shall not be unreasonably withheld or delayed; provided however, that either party may assign this SaaS Agreement to an acquirer of all or substantially all of the business of such party to which this SaaS Agreement relates, whether by merger, asset sale or otherwise or to any of its Affiliates. 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.

14.3 Notices. Except as otherwise 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 transmitted if sent by facsimile, provided that a copy of the notice is promptly sent by

another means specified in this section, or (c) when delivered if delivered personally or sent by express courier service. All notices shall be sent to the other party at the address set forth on the cover page of this SaaS Agreement.

14.4 Force Majeure. Each party will be excused from performance for any period during which, and to the extent that, such party or any subcontractor is prevented from performing any obligation or Service, in whole or in part, as a result of causes beyond its reasonable control, and without its fault or negligence, including without limitation, acts of God, strikes, lockouts, riots, acts of terrorism or war, epidemics, communication line failures, and power failures.

14.5 Waiver. No waiver shall be effective unless it is in writing and signed by the waiving party. The waiver by either party of any breach of this SaaS Agreement shall not constitute a waiver of any other or subsequent breach.

14.6 Severability. If any term of this SaaS Agreement is held to be invalid or unenforceable, that term shall be reformed to achieve as nearly as possible the same effect as the original term, and the remainder of this SaaS Agreement shall remain in full force.

14.7 Entire Agreement. This SaaS Agreement (including all Schedules and exhibits) contains the entire agreement of the parties and supersedes all previous oral and written communications by the parties, concerning the subject matter of this SaaS Agreement. This SaaS Agreement may be amended solely in a writing signed by both parties. Standard or printed terms contained in any purchase order or sales confirmation are deemed rejected and shall be void unless specifically accepted in writing by the party against whom their enforcement is sought; mere commencement of Services or payment against such forms shall not be deemed acceptance of the terms.

14.8 Survival. Section 3 "Restrictions", Sub-Section 5.2 "Invoice and Payment", Section 6 "Term and Termination", Section 9 "Limitations of Liability", Section 11 "Confidentiality", and Section 14 "General Provisions" of this SaaS Agreement shall survive the expiration or termination of this SaaS Agreement for any reason.

14.9 Publicity. SailPoint may include Customer's name and logo in its customer lists and on its website. Upon signing, SailPoint may issue a high-level press release announcing the relationship and the manner in which Customer will use the SailPoint solution. SailPoint shall coordinate its efforts with appropriate communications personnel in Customer's organisation to secure approval of the press release if necessary.

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

14.11 No Third Party Beneficiaries. This SaaS Agreement is an agreement between the parties, and confers no rights upon either party's employees, agents, contractors, partners or customers or upon any other person or entity.

14.12 Independent Contractor. 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.

14.13 Statistical Information. SailPoint may anonymously compile statistical information related to the performance of the SaaS Services for purposes of improving the SaaS Services, provided that such information does not identify Customer's data or include Customer's name.

14.14 Governing Law. Where the address of the Customer (as contained at the head of this Agreement or any Order hereto) is located in any of the following countries, then the laws of such country shall apply thereto: **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 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 shall not apply

14.15 Compliance with Laws. SailPoint shall comply with all applicable laws in connection with its delivery of the SaaS Services, including those laws related to data privacy, international communications, and the transmission of technical or personal data.

14.16 Dispute Resolution. Except with respect to any claim for the protection of a party's intellectual property rights, if a dispute arises between the parties relating to the interpretation or performance of this SaaS Agreement or the grounds for the termination hereof, the parties agree to hold a meeting within fifteen (15) days of written request by either party, attended by individuals with decision-making authority regarding the dispute, to attempt in good faith to negotiate a resolution of the dispute prior to pursuing other available remedies. If, within fifteen (15) days after such meeting, the parties have not succeeded in resolving the dispute, either party may protect its interests by any lawful means available to it.

14.17 Anti-Bribery/Corruption

(a) SailPoint shall ensure that, in relation to this SaaS Agreement and general business practices, it shall not engage in any activity, practice or conduct which may constitute an offence under any applicable Anti-Corruption Laws. In particular, SailPoint shall not offer, promise or pay to, or solicit or receive from any other person (including public and government officials) or company, any financial or other advantage which causes or is intended to cause another person to improperly perform their function or activities in order to secure or retain a business advantage. SailPoint shall further ensure that, unless allowed or required by local law, it shall not offer, promise or pay to any public government official any financial or other advantage in order to secure or retain a business advantage, including payment intended to induce officials to perform duties they are otherwise obligated to perform.

(b) As part of its internal measures to ensure compliance under this Section, SailPoint shall have in place and maintain policies and procedures to assess the risk of, monitor, and prevent the breaching of Anti-Corruption Laws. Where such policies are not published by SailPoint generally on its website or are otherwise made available generally, such policies and procedures shall be provided to Customer upon Customer's written request.

14.18 Signatures. This SaaS Agreement may be executed in multiple counterparts, each of which when executed will be an original, and all of which, when taken together, will constitute one agreement. Delivery of an executed counterpart of a signature page of this SaaS Agreement by facsimile or other electronic transmission (including via pdf) will be effective as delivery of a manually executed counterpart.

*** End of Page ***

EXAMPLE TEMPLATE – to be completed where Customer is ordering SaaS Services from SailPoint directly.

EXHIBIT A

SOFTWARE & PRICE SCHEDULE

This Schedule, effective upon the SaaS Agreement Effective Date, documents the SaaS Services (defined below) being purchased by the Customer under the terms and conditions of this SaaS Agreement.

[Page left intentionally blank]

EXHIBIT B

Premium IDaaS Support

1. Premium IDaaS Support

Premium Identity as a Service Support and Maintenance Services ("IDaaS Support") are included in the SaaS Services subscription in Exhibit A and entitle Customer to the following:

(a) Telephone or electronic support in order to help Customer locate and correct problems with the SaaS Services.
(b) Bug fixes and code corrections to correct malfunctions in order to bring such SaaS Services into substantial conformity with the operating specifications contained in the Documentation.
(c) All extensions, enhancements and other changes that SailPoint, at its sole discretion, makes or adds to the SaaS Services and which SailPoint furnishes, without charge, to all other subscribers of the SaaS Services.
(d) Up to five (5) dedicated contacts designated by Customer in writing that will have access to support services.

2. Response and Resolution Goals

- "Business Hours" 8am-6pm [GMT]/[GMT+1]/[CET] time, Monday to Friday, except local public holidays for non-severity 1 cases. For all severity 1 cases: 7 days a week at 24 hours a day coverage.
- "Fix" means the repair or replacement of Software component to remedy Problem.
- "Problem" means a defect in Software as defined in SailPoint's standard Software specification that significantly degrades such Software.
- "Respond" means acknowledgement via email of Problem received containing severity, priority, and other useful information.
- "Workaround" means a change in the procedures followed or data supplied by SailPoint to avoid a Problem without substantially impairing Customer's use of the SaaS Services.

Problem Severity	***Response Goals***	***Resolution Goals***
1. The production system / application is down, seriously impacted and there is no reasonable Workaround currently available	SailPoint will Respond within 1 clock hour.	Upon confirmation of receipt, SailPoint will begin continuous work on the Problem, and a Customer resource must be available at any time to assist with problem determination. SailPoint support will provide reasonable effort for Workaround or Fix within 24 hours, once the Problem is reproducible or once we have identified the defect. SailPoint may incorporate Fix in future release of the SaaS Services.
2. The system or 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 2 Business Hours.	SailPoint support will provide reasonable effort for Workaround or Fix within 7 business days, once the Problem is reproducible. SailPoint may incorporate Fix in future release of the SaaS Services.
3. The system or 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 8 Business Hours.	SailPoint support will provide reasonable effort for Workaround or Fix within 10 business days, once the Problem is reproducible. SailPoint may incorporate Fix in future release of the SaaS Services.

Problem Severity	*Response Goals*	*Resolution Goals*
4. Non-critical issues, general questions, enhancement requests or functionality that does not match documented specifications. (Example: General questions, basic help with understanding and using system and applications, etc.)	SailPoint will Respond within 12 Business Hours.	Resolution of Problem may appear in future release of the SaaS Services.

3. Accessing Support

SailPoint support offers several ways to resolve any technical difficulties. Online help can be accessed by clicking the "Help" tab when logged into the SaaS Services.

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

- Viewing updates to supported browsers, mobile operating systems and related software
- Accessing our knowledgebase, product documentation, training, technical articles, and FAQs

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

- Creating, updating and viewing cases, including adding attachments
- Submitting new product enhancements (Ideas)
- Support policy documentation
- Reporting status of cases

The support email address is support@sailpoint.com. The support phone number is 512-346-2000 or 1-888-472-4578.

*****End of Page*****

EXHIBIT C

SERVICE LEVEL AGREEMENT

The SaaS Services will achieve System Availability (as defined below) of at least 99.9% during each calendar month of the Subscription Term. "**System Availability**" means the number of minutes in a month that the key components of the SaaS Services in a Customer production environment are operational as a percentage of the total number of minutes in such month, excluding downtime resulting from:

(a) scheduled maintenance,

(b) events of Force Majeure,

(c) malicious attacks on the system,

(d) issues associated with the Customer's computing devices, local area networks or internet service provider connections, or

(e) inability to deliver services because of acts or omissions of Customer or any Identity Cube user.

SailPoint reserves the right to take the SaaS Services 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.

If SailPoint fails to meet System Availability in an individual month, upon written request by Customer within 30 days after the end of the month, SailPoint will issue a credit in Customer's next invoice in an amount equal to ten percent (10%) of the monthly fee for the affected SaaS Services for each 1% loss of System Availability below stated SLA per SaaS Service, up to a maximum of fifty percent (50%) of the Customer's monthly fee for the affected SaaS Services.

At Customer's election SailPoint shall provide a credit to Customer to be used for additional Identity Cubes or term extension or future SaaS Services renewals. In the event SailPoint fails to meet its obligations under the terms of this Service Level Agreement for three (3) consecutive months during any twelve (12) month period or five (5) months during a calendar year period, Customer shall have the option, in its sole discretion, to terminate this SaaS Agreement without penalty or further cost and SailPoint shall immediately repay to Customer all pre-paid amounts for any SaaS Services scheduled to be delivered after SailPoint's receipt of Customer's termination notice. The remedy stated in this paragraph is Customer's sole and exclusive remedy for interruption of SaaS Services and SailPoint's failure to meet System Availability.

Customer may enquire at any time as to SailPoint's compliance with the provisions of this Exhibit C by way of accessing SailPoint's general status website, located currently at http://status.identitynow.com

*****End of Page*****

SailPoint Technologies, Inc.,
Customer EU Data Processing Addendum

This Data Processing Addendum ("**DPA**"), forms part of the SaaS Agreement between SailPoint and Customer. All capitalised terms not defined in this DPA shall have the meanings set forth in the SaaS Agreement.

1. Definitions specific to this DPA

"**Affiliate**" 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%.

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

"**Customer Data**" means the data provided by or on behalf of the Customer (or its end users) to SailPoint via the SaaS.

"**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 SaaS 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 Data on behalf of a Data Controller.

"**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 SaaS 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) 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 the UK and 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.

"**SailPoint**" means SailPoint Technologies, Inc., a company incorporated under the laws of Delaware, United States of America, whose principal place of business is at 11120 Four Points Drive, Suite 100, Austin, Texas 78726, USA.

"**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 SaaS Services provided by SailPoint to Customer pursuant to the SaaS 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 SaaS Agreement or this DPA. Sub-processors may include third parties or SailPoint's Affiliates.

"**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.

2. 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 SaaS Agreement; and (ii) Customer is subject to European Data Protection Law.

2.2 Notwithstanding expiry or termination of the SaaS Agreement and subject to Section 10 (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.

3. 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 SaaS 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 SaaS 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 SaaS 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 SaaS 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 SaaS Agreement, SailPoint will Process Customer Personal Information upon the instruction of the Customer in accordance with the terms of the SaaS 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 SaaS 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 SaaS 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 SaaS 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 SaaS 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 SaaS Agreement, including to provide Personal Information to advisers or sub-processors as described below, or to the extent such disclosure is required by law.

4. 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 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.

5. 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** ("**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 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.

6. 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.

7. 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).

8. 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.

9. Return or Deletion of Customer Personal Information

On termination or expiration of the SaaS 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.

10. 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 (at Customer's expense) 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 SaaS 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.

11. Relationship with the SaaS Agreement

11.1 Except for the changes made by this DPA, the SaaS Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the SaaS 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 SaaS 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 SaaS Agreement. Without limiting either of the parties' obligations under the SaaS 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 SaaS Agreement as if it were liability to the Customer under the SaaS 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 SaaS Agreement against the SailPoint entity that is a party to the SaaS 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 SaaS 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 SaaS 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.

End of Page

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 to this Annex B.

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 Annex B;

(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. Variations

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.

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 SaaS Agreement which process Customer Personal Information upon the instruction of the Customer in accordance with the terms of the SaaS 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.

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 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 SaaS 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 SaaS 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 SaaS 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

1. 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.

2. 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.

*****End of Document*****