SCC AMENDMENT

This SCC Amendment ("**Amendment**") amends the current data processing terms governing the commercial agreement between SailPoint Technologies, Inc ("**SailPoint**") and Customer to insert name ("**Customer**"), pursuant to which Customer has procured SailPoint products and Services (together with any associated Order(s) and/or Statements of Work(s), (the "**Agreement**") between SailPoint and Customer. This Amendment is entered into as of the later of the dates beneath the parties' signatures below ("**Amendment Effective Date**"). Unless otherwise defined herein, capitalized terms used in this Amendment shall have the meaning as set forth in the Agreement.

IN WITNESS WHEREOF, the parties' authorised signatories have duly executed this Amendment as of the Amendment Effective Date.

Signatures

Customer to insert name	**SailPoint Technologies, Inc.**
By:	By: T A. Beck
Name: Customer to insert name of signatory	Name: Tom Beck
Title: Customer to insert title of signatory	Title: VP, Operations
Date: Customer to insert date of signature	Date: July 8, 2022

Recitals

WHEREAS, the European Commission published new Standard Contractual Clauses pursuant to European Commission Implementing Decision 2021/914/EU to address data transfers originating from the European Economic Area ("**EEA**"); and

WHEREAS, the parties now wish to amend the Data Processing Terms to replace the previous Standard Contractual Clauses pursuant to Commission Decision 2010/87/EU ("**2010 SCCs**") with the new Standard Contractual Clauses or, where the 2010 SCCs do not form part of the Agreement, to include the new Standard Contractual Clauses.

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the parties agree to amend the Data Processing Terms as follows:

1. Definitions

"**Customer**" means the Customer entity which is a party to the Agreement.

"**GDPR**" means either or both the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**") and the EU GDPR as it forms part of United Kingdom ("**UK**") law by virtue of the UK General Data Protection Regulation, tailored by the Data Protection Act 2018 ("**UK GDPR**"), as the context may require.

"**Data Processing Terms**" means the data processing terms executed between the parties in either a Data Processing Agreement, a Data Processing Exhibit, Data Processing Terms, or another similarly titled exhibit to the Agreement or within the body of the Agreement.

"**Order**" means a schedule, quote or quotation, statement of work, or other document(s) by which Customer (or a partner on Customer's behalf) orders Services governed by the Agreement.

"**Other Services**" means all technical and non-technical consulting and advisory services identified in an Order as Professional Services or Training Services and performed or delivered by SailPoint under the Agreement. Other Services are not available or provided on a work-for-hire basis. For purposes of clarity, "Other Services" does not include the SaaS Services, SaaS Support or Software Support.

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

"**Restricted Country**" means: (i) where the EU GDPR applies, a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a country outside the UK which is not based on adequacy regulations pursuant to Section 17A of the UK Data Protection Act 2018; and (iii) where the Swiss Federal Act on Data Protection of June 19, 1992 applies, a country outside Switzerland which has not been recognized to provide an adequate level of protection by the Federal Data Protection and Information Commissioner.

"**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Personal Data from the EEA to a Restricted Country; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to a Restricted Country; and (iii) where the Swiss Federal Act on Data Protection of June 19, 1992 applies, a transfer of Personal Data from Switzerland to a Restricted Country.

"**SaaS Support**" means SailPoint's Support and Maintenance Services for SaaS Services as described in the SailPoint Support and Maintenance Policy found at the Customer Agreements landing page under Associated Documentation on SailPoint's website at https://www.sailpoint.com/legal/.

"**Services**" means the services provided by SailPoint to Customer pursuant to the Agreement, which may include: (i) support and maintenance services for its on-premises Software; (ii) SaaS Services; and (iii) Other Services provided by SailPoint to Customer pursuant to the Agreement.

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

"**Software Support**" means SailPoint's Support and Maintenance Services for Software in accordance with the terms and conditions of the applicable agreement between a customer and SailPoint (including the applicable Order) and described in the SailPoint Support and Maintenance Policy found under Associated Documentation on SailPoint's website at https://www.sailpoint.com/legal/.

"**Standard Contractual Clauses**" means (i) where the EU GDPR applies, the clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, the EU SCCs as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as issued by the UK Information Commissioner's Office ("**UK Addendum**") and attached hereto as Schedule A.

"**Sub-processor**" or "**Subprocessor**" means any entity engaged by SailPoint, including its Affiliates, to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or the Data Processing Terms.

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

2. Standard Contractual Clauses

2.1. **Customer SCCs.** Where SailPoint has a Subprocessor that is located in a Restricted Country, SailPoint has, or will by 27 December 2022 for EU Personal Data and by 21 March 2024 for UK Personal Data, implemented the Standard Contractual Clauses for any Restricted Transfers of Personal Data from SailPoint (as "data exporter") to such Subprocessor (as "data importers").

2.2. **Customer SCCs.** Where SailPoint is located in a Restricted Country, the Standard Contractual Clauses will apply to any Restricted Transfers from Customer and Customer Affiliates (each as "data exporter") to SailPoint (as "data importer") as follows:

2.2.1. **EU Personal Data.** In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module 2 applies;

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

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes will be in accordance with the notification process set out Subprocessor provisions of the Data Processing Terms. SailPoint's current list of Sub-processors is located on SailPoint's website at https://www.sailpoint.com/legal/sub-processors;

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

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

(vi) in Clause 18(b), disputes shall be resolved before the courts specified in the Agreement, provided these courts are located in an EU Member State, otherwise those courts shall be the courts of the Netherlands;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this Amendment; and

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this Amendment;

2.2.2. UK Personal Data. The parties agree that the following provisions shall apply with respect to data transfers that are governed by the UK GDPR when (i) SailPoint Processes Personal Data on the behalf of Customer as a Processor in the course of providing Services pursuant to the Agreement; and (ii) Customer is subject to UK Data Protection Laws as defined in the UK Addendum:

(i) To the extent that SailPoint Processes any Personal Data from the UK and transfers such Personal Data outside of the UK to countries not deemed by the UK Information Commissioner's Office to provide an adequate level of data protection, the parties agree to comply with the EU SCCs in accordance with this Amendment, as amended by the UK Addendum attached hereto as Schedule A;

(ii) Execution of this Amendment is deemed acceptance and execution of the attached UK Addendum.

2.2.3. Swiss Personal Data. The parties agree that the following provisions shall apply with respect to data transfers that are governed by the Federal Act on Data Protection ("FADP"), when (i) SailPoint Processes Personal Data on the behalf of Customer as a Processor in the course of providing Services pursuant to the Agreement; and (ii) Customer is subject to FDAP:

(i) To the extent that SailPoint Processes any Personal Data subject to the FADP, the parties agree to comply with the EU SCCs, as amended by the following provisions of this clause 2.2.3;

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

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

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

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

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

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

2.3. Prior SCCs. If the Data Processing Terms already incorporate the 2010 SCCs, this Amendment will supersede and replace all prior 2010 SCCs as of the Amendment Effective Date. All references to the 2010 SCCs shall be replaced with references to the Standard Contractual Clauses.

3. Clarifications to the Standard Contractual Clauses

3.1. Audits. SailPoint will allow Customer to conduct audits as described in the Standard Contractual Clauses in accordance with the audit provisions of the Data Processing Terms.

3.2. Subprocessors. Customer consents to SailPoint appointing Subprocessors in accordance with the Subprocessor provisions of the Data Processing Terms, and Customer may exercise its right to object to Subprocessors under the Standard Contractual Clauses in the manner set out in the Subprocessor provisions of the Data Processing Terms.

3.3. Return and Deletion of Personal Data. SailPoint shall return and delete Customer's data in accordance with the return and deletion provisions of the Data Processing Terms.

3.4. Fees and costs. Customer agrees that any assistance that SailPoint provides to Customer under the Standard Contractual Clauses shall be provided under the relevant provisions of the Data Processing Terms.

3.5. Conflict. Nothing in this Clause 3 varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses. If any provision of this Amendment contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

4. General Provisions. Except as amended hereby, the Data Processing Terms shall remain in full force and effect. This Amendment may be executed electronically and/or in counterpart originals, each of which shall be deemed an original instrument for all purposes, but all of which shall comprise one and the same instrument.

ANNEX I – Details of Processing

This Annex forms part of the Data Processing Terms and Clauses and must be completed and signed by the parties.

A. LIST OF PARTIES

Data exporter(s):

Name: Customer to insert name

Address: Customer to insert address

Contact person's name, position and contact details:

Customer to insert its Data Protection Officer (DPO) or head of privacy (not necessarily the signatory b

Activities relevant to the data transferred under these Clauses:

For any on-premises software: SailPoint's Software Support and Other Services (e.g., program planning, software deployment assistance, interface adapter efforts, and/or formal or non-formal software training).

For any SaaS solutions: SailPoint's SaaS Services, SaaS Support, and Other Services (e.g., implementation services, implementation support, best practices consultations, integration efforts, and training and education services).

Signature:

Date: Customer to insert date of signature

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

Name: SailPoint Technologies, Inc

Address: 11120 Four Points Drive, Suite 100, Austin, Texas 78726, USA

Contact person's name, position and contact details:

SailPoint's Data Protection Officer:
Dr. Felix Wittern
Partner, Fieldfisher
Hamburg, Germany
privacy@sailpoint.com

Activities relevant to the data transferred under these Clauses: Same as listed above for data exporter.

Signature: A. Beck

Date: July 8, 2022

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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

Categories of personal data transferred

Identification and contact data (e.g., name, address, title, contact details), employment details (e.g., job title, role, manager), and/or IT information (e.g., entitlements, IP addresses, usage data, cookies data, and geolocation).

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

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

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

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

Nature of the processing

To provide Services to Customer under the Agreement.

Purpose(s) of the data transfer and further processing

The provision of Services by SailPoint under the Agreement.

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

The Customer Personal Information Processed by SailPoint will be retained for the duration of the Processing by SailPoint in the context of the provision of Services under the Agreement, and thereafter in order to comply with applicable law, including Data Protection Laws.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

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

Nature of sub-processing:
To assist SailPoint in providing solutions and other Services to Customer under the Agreement.

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

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13

Customer to insert competent supervisory authority here

End of Annex I

ANNEX II– Technical and Organisational Measures including Technical and Organisational Measures to ensure the Security of the Data

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

Application to Transfers:

Cross-border transfers by Customer to SailPoint relate to SailPoint's (1) SaaS Support and Software Support and/or (2) SaaS Services and Other Services. Customer controls what data SailPoint has access to for these purposes. As such, SailPoint's technical and organisational measures, as a whole, concern its access to transferred data.

Technical and Organisational 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.

1. Security Program

a. ISO27001-based Information Security Management System (ISMS): SailPoint shall maintain an ISMS risk-based security program to systematically manage and protect the organisation's business information and the information of its customers and partners.
b. Security Governance Committee: SailPoint shall maintain a security committee comprised of leaders across all business units that oversees the company's security program. This committee shall meet monthly to review the operational status of the ISMS (including risks, threats, remediation actions, and other security-related issues) and drive continuous security improvement throughout the business.
c. Security incident response policy: SailPoint shall maintain policies and procedures to (1) investigate and respond to security incidents, including procedures to assess the threat of relevant vulnerabilities or security incidents using defined incident classifications and categorisations and (2) establish remediation and mitigation actions for events, including artifact and evidence collection procedures and defined remediation steps.
d. Policy maintenance: All security and privacy related policies shall be documented, reviewed, updated and approved by management at least annually to ensure they remain consistent with best practices, legal and regulatory requirements and industry standards.
e. Communication and commitment: Security and privacy policies and procedures shall be published and effectively communicated to all personnel and relevant subcontractors. Security shall be addressed at the highest levels of the company with executive management regularly discussing security issues and leading company-wide security initiatives.

2. Personnel Security

a. Background screening: Personnel who have access to Customer Personal Information or the equipment on which it is stored shall be subject to background screening (as allowed by local laws and regulations) that shall include verification of identity, right to work and academic degrees and a check of criminal records, sex offender registries and prohibited/denied party lists.
b. Confidentiality obligations: Personnel who have access to Customer Personal Information shall be subject to a binding contractual obligation with SailPoint to keep the Customer Personal Information confidential.
c. Security awareness training: Personnel shall receive training upon hire and at least annually thereafter covering security best practices and privacy principles.
d. Code of conduct: SailPoint shall maintain a code of business conduct policy and compliance program to ensure ethical behaviour and compliance with applicable laws and regulations.

3. Third-Party Security

a. Screening: SailPoint shall maintain policies and procedures to ensure that all new suppliers, SaaS applications, IT Software, and IT service solutions are subject to reasonable due diligence to confirm their ability to meet corporate security and compliance requirements as well as business objectives.
b. Contractual obligations: SailPoint shall ensure that contractual agreements with suppliers include confidentiality and privacy provisions as appropriate to protect SailPoint's interests and to ensure SailPoint can meet its security and privacy obligations to customers, partners, employees, regulators and other stakeholders.
c. Monitoring: SailPoint shall periodically review existing third-party suppliers to ensure the supplier complies with contractual terms, including any security and availability requirements. The monitoring program shall review suppliers at least annually (regardless of length of contractual term) to confirm that the supplier/solution is still meeting the company's objectives and the supplier's performance, security, and compliance postures are still appropriate given the type of access and classification of data being accessed, controls necessary to protect data, and applicable legal and regulatory requirements.

4. Physical Security

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

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

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

5. Solution Security

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

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

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

6. Operational Security

a. Access controls: SailPoint shall maintain policies, procedures, and logical controls to establish access authorisations for employees and third parties to limit access to properly authorized personnel and to prevent unauthorised access. Such controls shall include:
   i. requiring unique user IDs to identify any user who accesses systems or data;
   ii. managing privileged access credentials in a privileged account management (PAM) system;
   iii. communicating passwords separately from user IDs;
   iv. ensuring that user passwords are (1) changed at regular intervals; (2) of sufficient length and complexity; (3) stored in an encrypted format; (4) subject to reuse limitations; and (5) not assigned to other users, even at a different time; and
   v. automatically locking out users' IDs when a number of erroneous passwords have been entered.

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

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

d. Encryption: SailPoint shall use industry-standard strong encryption methods to protect data in transit and at rest as appropriate to the sensitivity of the data and the risks associated with loss; all laptops and other removable media, including backup tapes, on which Customer Personal Information is stored shall be encrypted.

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

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

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

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

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

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

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

End of Annex II

ANNEX III – List of Subprocessors

This Annex does not require completion since specific authorisation of sub-processors (Clause 9(a), Option 1) has not been selected and the SailPoint current list of processors is detailed in clause 2.2.1 (iii) of this Amendment.

End of Annex III

Schedule A – UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Information Commissioner under S119A(1) Data Protection Act 2018

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The Effective Date as defined in the Amendment	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: as detailed in Annex 1A of the EU SCCs annexed to the Amendment Trading name (if different): Customer to complete if relevant – if not, lea Main address (if a company registered address): as detailed in Annex 1A of the EU SCCs annexed to the Amendment Official registration number (if any) (company number or similar identifier): Customer to complete if relevant – if not, lea	Full legal name: as detailed in Annex 1A of the EU SCCs annexed to the Amendment Trading name (if different): N/A Main address (if a company registered address): as detailed in Annex 1A of the EU SCCs annexed to the Amendment Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): as detailed in Annex 1A of the EU SCCs annexed to the Amendment Job Title: as detailed in Annex 1A of the EU SCCs annexed to the Amendment Contact details including email: as detailed in Annex 1A of the EU SCCs annexed to the Amendment	Full Name (optional): as detailed in Annex 1A of the EU SCCs annexed to the Amendment Job Title: as detailed in Annex 1A of the EU SCCs annexed to the Amendment Contact details including email: as detailed in Annex 1A of the EU SCCs annexed to the Amendment

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective Date as defined in the Amendment Reference (if any): N/A Other identifier (if any): N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: SailPoint Technologies, Inc., and Customer as detailed in the Data Processing Terms
Annex 1B: Description of Transfer: See Annex 1B of EU SCCs annexed to the Amendment
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex 2 of EU SCCs annexed to the Amendment
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex 3 of EU SCCs annexed to the Amendment

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK

	GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a. its direct costs of performing its obligations under the Addendum; and/or

b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

End of Schedule A