DATA PROCESSING ADDENDUM

(Customer)

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

IN WITNESS WHEREOF, SailPoint Technologies, Inc. ("**SailPoint**") and Customer to insert name ("**Customer**") (together, the "**parties**" to this DPA and the Agreement) have caused this DPA to be executed by their authorized representatives:

Signatures

Customer to insert name ("**Customer**")	**SailPoint Technologies, Inc.**
By: _____	By: Tom 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: September 9, 2022

1. Definitions

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

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

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

"**Customer Data**" has the meaning set forth in the Agreement (if any). To the extent that that there is no meaning set forth in the Agreement, "Customer Data" for the purposes of this DPA means any data of any type that is submitted by or on behalf of Customer to SailPoint in connection with the Services.

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

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Information under the Agreement, provided that such laws are no more prescriptive than the General Data Protection Regulation or any other law specifically referenced herein.

"**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.

"**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.

"**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 Customer Personal Information, whether or not by automatic means.

"**Professional Services**" means consulting services provided by SailPoint to Customer that support Customer's deployment, extension and use of SaaS Services and include, but are not limited to, implementation services,

implementation support, best practices consultations, and integration efforts as further described in, and subject to, the Agreement (including the applicable Order).

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

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

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

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

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

"**Software**" means the object code version of the specific SailPoint computer software licensed to Customer, including any updates, modifications, new versions or releases of the Software provided by SailPoint to Customer over time.

"**Software Support**" means the Support and Maintenance Services provided for Software by SailPoint to Customer 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/.

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

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

1.2. Capitalised terms used in this DPA that are not defined in this Section 1 (Definitions) shall have the meaning ascribed to them elsewhere in this DPA and/or the Agreement or in applicable Data Protection Laws unless otherwise specified.

2. Jurisdiction-Specific Addenda

2.1. Attached to this DPA are Addenda that provide terms specific to the Processing of Customer Personal Information arising out of specific legal requirements from particular jurisdictions. In the event that Customer Personal Information is Processed from one or more of these jurisdictions, and the applicable requirements are not already covered in this DPA, then the terms in the respective Addendum attached hereto shall apply.In the event of a conflict between the Agreement or this DPA and an Addendum, the Addendum applicable to Customer Personal Information from the relevant jurisdiction shall control with respect to Customer Personal Information from that relevant jurisdiction, and solely with regard to the portion of the provision in conflict.

2.2. Customer has sole responsibility for informing SailPoint when Customer Personal Information is within the scope of one or more Addenda. Customer confirms that, at the time of execution of this DPA, Customer Personal Information is within scope of the following Addenda:

- ☐ **California Consumer Privacy Act Addendum**
- ☐ **European Economic Area Addendum**
- ☐ **Switzerland Addendum**
- ☐ **UK Addendum**

2.3. In the event Customer believes additional Addenda should apply, Customer has the sole responsibility for notifying SailPoint and working with SailPoint to effectuate such Addenda.

3. Updates to DPA. In the event of changes to applicable Data Protection Laws, including, but not limited to, the amendment, revision, or introduction of new laws, regulations, or other legally binding requirements to which either party is subject, the parties agree to revisit the terms of this DPA, and negotiate any appropriate or necessary updates in good faith, including the addition, amendment, or replacement of any Addenda.

4. Roles and Scope of Processing

4.1. Customer Processing of Personal Information. Customer: (i) agrees that it will comply with its obligations under Data Protection Laws in respect of its Processing of Personal Information and any Processing instructions it issues

to SailPoint; and (ii) represents and warrants that it has provided all fair processing notices and obtained all consents and rights necessary under Data Protection Laws for SailPoint to Process Personal Information and provide the Services pursuant to the Agreement and this DPA.

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

4.3. **Details of Data Processing**.

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

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

(b) Categories of Personal Information transferred:

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

(c) Sensitive data transferred (if applicable):

None.

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

For 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.

(e) Nature of the processing

To provide Services to Customer under the Agreement.

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

The provision of Services by SailPoint under the Agreement.

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

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

5. Sub-processing

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

5.2. **Sub-processor Obligations**. SailPoint will: (i) not engage a Sub-processor unless SailPoint enters into a written agreement with the Sub-processor which contain obligations that are at least as restrictive as those set out in this DPA; and (ii) remain responsible for its compliance with the obligations of this DPA and for any failure by a Sub-processor engaged by SailPoint to fulfil its data protection obligations under the applicable Data Protection Laws.

6. Security

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

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

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

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

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

7. Security Reports and Audits

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

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

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

8. International Operations

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

9. Additional Security

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

9.2. **Security Incident Response**. SailPoint shall: (i) taking into account the nature of SailPoint's Processing of Customer Personal Information and the information available to SailPoint, notify Customer of a Security Incident that it becomes aware of, without undue delay; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.3. **Notification**. Customer acknowledges that SailPoint will not assess the contents of Customer Personal Information in order to identify information subject to any specific legal requirements. Customer is solely responsible to comply with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incidents as required by Data Protection Laws. Unless otherwise required under Data Protection Laws, the parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected data subjects and/or notices to the relevant supervisory authorities.

10. Relationship with the Agreement

10.1. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Information.

10.2. Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement. Without limiting either of the parties' obligations under the Agreement, Customer agrees that any regulatory penalties incurred by SailPoint that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce SailPoint's liability under the Agreement as if it were liability to the Customer under the Agreement.

10.3. Any claims against SailPoint or its Affiliates under this DPA shall only be brought by the Customer entity that is a party to the Agreement against the SailPoint entity that is a party to the Agreement. In no event shall this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority.

10.4. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

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

Annex A – Security Measures

SailPoint Data Security Program

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

1. Security Program

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

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

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

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

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

2. Personnel Security

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

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

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

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

3. Third-Party Security

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

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

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

4. Physical Security

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

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

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

5. Solution Security

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

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

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

6. Operational Security

a. Access controls: SailPoint shall maintain policies, procedures, and logical controls to establish access authorisations for employees and third parties to limit access to properly 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.

California Consumer Privacy Act Addendum

1. Scope

This Addendum shall apply in the event that SailPoint Processes Customer Personal Information of California residents.

2. Definitions

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

2.2 All words or phrases used herein not defined in the DPA will have the meaning assigned to them in the CCPA.

3. Terms

3.1 SailPoint will not sell any Customer Personal Information received from Customer.

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

4. Cooperation

4.1 Taking into account the nature of the Processing, SailPoint shall (at Customer's request and expense) provide reasonable cooperation to assist Customer to respond to any requests from data subjects in relation to their data subject rights under Data Protection Laws or applicable regulatory authorities relating to the Processing of Customer Personal Information under the Agreement. In the event that any request from data subjects or applicable regulatory authorities is made directly to SailPoint, SailPoint shall not respond to such communication directly without Customer's prior authorisation other than to inform the requestor that SailPoint is not authorised to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to 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.

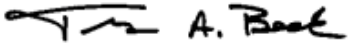
4.2 If a law enforcement agency sends SailPoint a demand for Customer Personal Information (e.g., a subpoena or court order), SailPoint will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, SailPoint may provide Customer's contact information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

European Economic Area Addendum

IN WITNESS WHEREOF, SailPoint Technologies, Inc. ("**SailPoint**") and Customer to insert name ("**Customer**") (together, the "**parties**") have caused this Addendum to be executed by their authorized representative.

WHEREAS, by executing this Addendum, the parties satisfy any signature requirement in "Annex 1: List of Parties" to the Standard Contractual Clauses attached hereto and discussed below.

Signatures

Customer to insert name	**SailPoint Technologies, Inc.**
By:	By: 
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: September 9, 2022

1. Scope

This Addendum (also "**EEA Addendum**") shall apply in the event that: (i) SailPoint Processes Customer Personal Information on the behalf of Customer as a Processor in the course of providing Services pursuant to the Agreement; and (ii) Customer is subject to European Data Protection Law and acts as a Controller thereunder.

2. Definitions

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

2.2 "**European Data Protection Law**" means: (i) the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**") as implemented by countries within the EEA; (ii) the European Union e-Privacy Directive 2002/58/EC as implemented by countries within the EEA; 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) and (ii) above.

2.3 "**Model Clauses**," "**SCCs**," or "**Clauses**" means the Standard Contractual Clauses for Processors as approved by the European Commission in the form set out in Schedule A to this Addendum.

2.4 All terms used herein not defined in the DPA will have the meaning assigned to them in the applicable European Data Protection Law. All references to Data Protection Law or laws in the DPA shall be read in the context of EU or Member State law for the purpose of this Addendum.

3. Sub-processors.

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

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

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

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

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

(d) The parties agree that any non-response by the Customer during the Review Period will be taken as the Customer's approval of additional or replacement Sub-processors, where Customer continues to use the Services after the Review Period has lapsed. CLAUSE 9(A) OF THE SCCS AND THIS CLAUSE 3.2 STATE THE ENTIRE LIABILITY OF SAILPOINT AND THE SOLE REMEDY FOR CUSTOMER IN CONNECTION WITH ANY OBJECTION BY CUSTOMER TO AN INTENDED ADDITIONAL OR REPLACEMENT SUB-PROCESSOR WHO WILL PROCESS CUSTOMER PERSONAL INFORMATION.

4. Cooperation

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

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

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

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

4.5 Customer acknowledges that SailPoint may be required under European Data Protection Law to: (i) collect and maintain records of certain information, including the name and contact details of each Processor and/or Controller on behalf of which SailPoint is acting and, where applicable, of such Processor's or Controller's local representative and data protection officer; and (ii) make such information available to the supervisory authorities. Accordingly, if European Data Protection Law applies to the Processing of Customer Personal Information, Customer will, where requested, provide such information to SailPoint, and will ensure that all information provided is kept accurate and up-to-date.

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

5. International Transfers

5.1 To the extent that SailPoint Processes any Customer Personal Information from the EEA and transfers such Customer Personal Information outside of the EEA 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 found in Schedule A of this Addendum. 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).

5.2 The parties agree that the data export solution identified in Section 5.1 (International Transfers) 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, in which event, Customer shall take any action (which may include execution of documents) required to give effect to such solution and the alternative transfer mechanism will apply instead (but only to the extent such alternative transfer mechanism extends to the jurisdictions to which Customer Personal Information is transferred).

6. Supervision and Governance

6.1 In respect of, and as set forth in, Clause 13(a) of the SCCs:

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority;

(b) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority; and

(c) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

6.2 In respect of Annex I, Section C of the SCCs, the competent supervisory authority is:

Customer to insert competent supervisory authority here

7. Annex I: List of Parties

7.1 In respect of Annex 1: List of Parties of the SCCs, the requisite information is as follows:

(a) Data exporter(s):

Name: Customer to insert name
Address: Customer to insert address here
Contact person's name, position and contact details:

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

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 and date: Please see the first page of this Addendum.
Role (controller/processor): Controller

(b) Data importer(s):

Name: SailPoint Technologies, Inc.
Address: 11120 Four Points Drive, Suite 100, Austin, Texas 78726, USA
Contact person's name, position and contact details:

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

Activities relevant to the data transferred under these Clauses:

Same as listed above for data exporter.

Signature and date: Please see the first page of this Addendum.
Role (controller/processor): Processor

8. ADDITIONAL OBLIGATIONS

8.1 In respect of Clause 8.5 of the SCCs, the Agreement may specify the time period during which the Customer must request to have continued access to its Customer Personal Information after the end of the provision of the Services. Should the Customer make a request to have continued access to its Customer Personal Information, SailPoint will, after a recovery period of up to 30 days following such expiry or termination, comply with this instruction as soon as reasonably practicable, where technically feasible. Customer shall be responsible for retrieving any remaining Customer Personal Information it wishes to retain before the end of the recovery period. SailPoint shall not be required to delete or return Customer Personal Information to the extent: (i) SailPoint is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Personal Information; and/or (ii), Customer Personal Information it has archived on back-up systems, which Customer Personal Information SailPoint shall securely isolate and protect from any further processing, except to the extent required by applicable law.

8.2 Customer acknowledges that the technical and organisational measures in Annex II to Schedule A attached hereto are subject to technical progress and development and that SailPoint may update or modify the technical and organisational 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.

Schedule A - Model Clauses

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing)not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for

attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors pursuant to the time period established by the Parties in the European Economic Area Addendum, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-

material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements maybe considered as part of an overall assessment. Such elements may include relevant and documented practicalexperience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whethertheir practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Member State of the competent supervisory authority identified pursuant to Annex I, Section C below.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Member State of the competent supervisory authority identified pursuant to Annex I, Section C below.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Please see Section 7 of the EEA Addendum, which sets forth the parties' information.

B. DESCRIPTION OF TRANSFER

Please see Section 4.3 (Details of Data Processing) of the DPA for details of the transfer(s).

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

Please see Section 6 of the EEA Addendum, which sets forth the competent supervisory authority.

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

Technical and Organisational Measures:

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

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.

ANNEX III – LIST OF SUB-PROCESSORS

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 5.1 of this DPA.

Switzerland Addendum

This Addendum applies to and is a part of the New EU Commission Standard Contractual Clauses (Module 2 Controller to Processor) (the "**Clauses**") and European Economic Area Addendum ("**EEA Addendum**"), agreed between Customer and the SailPoint (together, the "**parties**").

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**"), e.g. personal data transferred by a data exporter from Switzerland to a data importer outside of Switzerland (including personal data located in Switzerland that a data exporter makes accessible to the data importer) (the "**Swiss Personal Data**"):

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

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

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

(iv) References to Member State(s), the EU and the EEA shall be deemed to include Switzerland; and

(v) Where the Clauses use terms that are defined in the EU General Data Protection Regulation 2016/679, those terms shall be deemed to have the meaning as the equivalent terms are defined in the FADP.

The list of data subjects and categories of data indicated in Annex I. B. to the Clauses shall not be deemed to restrict the application of the Clauses to the Swiss Personal Data.

IN WITNESS WHEREOF, SailPoint Technologies, Inc. ("**SailPoint**") and Customer to insert name ("**Customer**") (together, the "**parties**") have caused this Addendum to be executed by their authorized representative:

Data importer:	Data exporter:
SailPoint Technologies, Inc.	**Customer:** Customer to insert name
By: Tom A. Beck	By:
Name: Tom Beck	Name: Customer to insert name of signatory
Title: VP, Operations	Title: Customer to insert title of signatory
Date: September 9, 2022	Date: Customer to insert date of signature

UK Addendum

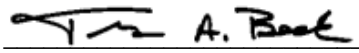
This Addendum applies to and is a part of the New EU Commission Standard Contractual Clauses (Module 2 Controller to Processor) and European Economic Area Addendum ("**EEA Addendum**") agreed between Customer and SailPoint (together, the "**parties**").

The parties agree that the following provisions shall apply with respect to data transfers that are governed by the UK General Data Protection Regulation, tailored by the Data Protection Act 2018 ("**UK GDPR**"), when (i) SailPoint Processes Customer Personal Information on the behalf of Customer as a Processor in the course of providing Services pursuant to the Agreement; and (ii) Customer is subject to UK Data Protection Law and acts as a Controller thereunder:

(i) To the extent that SailPoint Processes any Customer Personal Information from the UK and transfers such Customer Personal Information 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 Model Clauses found in Schedule A of the EEA Addendum executed by the Parties, as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses attached hereto as Schedule A;

(ii) Execution of this UK Addendum is deemed acceptance and execution of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses attached hereto as Schedule A;

IN WITNESS WHEREOF, SailPoint Technologies, Inc. ("**SailPoint**") and Customer to insert name ("**Customer**") (together, the "**parties**") have caused this Addendum to be executed by their authorized representative:

Data importer:	Data exporter:
SailPoint Technologies, Inc.	**Customer:** Customer to insert name
By: 	By: _____
Name: Tom Beck	Name: Customer to insert name of signatory
Title: VP, Operations	Title: Customer to insert title of signatory
Date: September 9, 2022	Date: Customer to insert date of signature

Schedule A

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 DPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Customer as detailed in clause 7.1 (a) of the EEA Addendum Trading name (if different): Customer to complete if relevant – if not, Main address (if a company registered address): as detailed in clause 7.1 (a) of the EEA Addendum Official registration number (if any) (company number or similar identifier): Customer to complete if relevant – if not,	Full legal name: SailPoint as detailed in clause 7.1 (b) of the EEA Addendum Trading name (if different): N/A Main address (if a company registered address): as detailed in clause 7.1 (b) of the EEA Addendum Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): as detailed in clause 7.1 (a) of the EEA Addendum Job Title: as detailed in clause 7.1 (a) of the EEA Addendum Contact details including email: as detailed in clause 7.1 (a) of the EEA Addendum	Full Name (optional): as detailed in clause 7.1 (b) of the EEA Addendum Job Title: as detailed in clause 7.1 (b) of the EEA Addendum Contact details including email: as detailed in clause 7.1 (b) of the EEA Addendum

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 DPA 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 DPA
Annex 1B: Description of Transfer: See Annex 1B of EU SCCs
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex 2 of EU SCCs
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex 3 of EU SCCs

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.