SailPoint Technologies, Inc.,
SaaS Customer EU Data Processing Addendum (v11102020)

This SaaS Customer EU 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, the parties have caused this DPA to be executed by their authorized representative:

SailPoint Technologies, Inc.	**Customer: _____**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

1. Definitions

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

"**Affiliate**" means an entity that controls, is controlled by or shares common control with a party, where such control arises from either (a) a direct or indirect ownership interest of more than 50% or (b) the power to direct or cause the direction of the management and policies, whether through the ownership of voting stock by contract, or otherwise, equal to that provided by a direct or indirect ownership of more than 50%.

"**Agreement**" means the SaaS Agreement.

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

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

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

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

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Information under the Agreement, including, but not limited to, (where applicable) European Data Protection Law and/or the CCPA.

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

"**European Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**") as implemented by countries within the EEA; (ii) the European Union e-Privacy Directive 2002/58/EC as implemented by countries within the EEA;and/or (iii) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i) through (ii) above, including by the UK and Switzerland.

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

"**Personal Information**" means: any information (i) relating to an identified or identifiable natural person; or (ii) defined as "personally identifiable information", "personal information", "personal data" or similar terms, as such terms are defined under Data Protection Laws.

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

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

"**Security Incident**" means any unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Personal Information on systems managed by or otherwise controlled by SailPoint but does not include any Unsuccessful Security Incident.

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

"**Services**" means the SaaS Service provided by SailPoint to Customer pursuant to the Agreement.

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

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

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

2. Scope and Applicability of this DPA

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

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

3. Roles and Scope of Processing

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

3.2 **Customer Processing of Personal Information**. Customer agrees that: (i) it will comply with its obligations under Data Protection Laws in respect of its Processing of Personal Information and any Processing instructions it issues to SailPoint; and (ii) it has provided all fair processing notices and obtained all consents and rights necessary under Data Protection Laws for SailPoint to Process Personal Information and provide the Services pursuant to the Agreement and this DPA. If European Data Protection Law applies to the Processing of Customer Personal Information and Customer is itself a Data Processor, Customer warrants to SailPoint that Customer's instructions and actions with respect to that Customer Personal Information, including its appointment of SailPoint as another Data Processor, have been authorised by the relevant Data Controller.

3.3 **Customer Instructions**. SailPoint will Process Customer Personal Information only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions, and applicable Data Protection Laws. The parties agree that this DPA and the Agreement set out the Customer's complete and final instructions to SailPoint in relation to the Processing of Customer Personal Information by SailPoint. Additional Processing outside the scope of these instructions (if any) will require prior written agreement between Customer and SailPoint.

3.4 **Details of Data Processing.**

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

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

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

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

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

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

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

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

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

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

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

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

3.5 **Access, Use or Sell**.

(a) SailPoint will not: (i) sell any Customer Personal Information received from Customer; or (ii) retain, access, disclose or use Customer Personal Information, provided by or collected on behalf of Customer for any purpose except as necessary to maintain or provide the Services specified in the Agreement and this DPA, or as necessary to comply with the law or binding order of a governmental body, including retaining, accessing, disclosing or using the Customer Information for a commercial purpose other than providing the Services specified in the Agreement.

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

4. Sub-processing

4.1 **Authorized Sub-processors**. Customer agrees that SailPoint may engage Sub-processors to Process Customer Personal Information on Customer's behalf. The Sub-processors currently engaged by SailPoint and authorized by Customer are listed on SailPoint's website at https://www.sailpoint.com/legal/sub-processors.

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

4.3 **Changes to Sub-processors**.

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

(b) Customer acknowledges and agrees that: (a) it will make every effort to provide SailPoint with its approval of SailPoint's Request within the Review Period (such approval not to be unreasonably withheld); and (b) any objections raised by Customer during the Review Period may only be based on reasonable grounds and only with respect to data protection concerns.

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

5. Security

5.1 **Security Measures**. Taking into account the nature of the Processing, SailPoint shall implement and maintain appropriate technical and 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 SaaS Data Security Program as described on SailPoint's website at https://www.sailpoint.com/legal/customer-agreements **the "Security Measures")**.

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

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

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

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

5.4 **Customer's Security Assessment.** Customer is responsible for reviewing the Security Measures and evaluating for itself whether the Services and the Security Measures and SailPoint's

commitments under this Section 5 (Security) and Section 8 (Additional Security) will meet Customer's needs, including with respect to any obligations of Customer under Data Protection Laws as applicable.

6. Security Reports and Audits

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

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

6.3 If Customer reasonably believes that the information provided pursuant to Sections 6.1 and/or 6.2 is insufficient to demonstrate compliance with this DPA, SailPoint will allow an audit by Customer (or auditors appointed by Customer and reasonably acceptable to SailPoint) in relation to SailPoint's Processing of Customer Personal Information. Any such audit will be at Customer's expense, with reasonable advance notice, conducted during normal business hours no more than once every 12 months and subject to SailPoint's reasonable security and confidentiality requirements and provided that the exercise of rights under this Section 6.3 would not infringe Data Protection Laws.

7. International Transfers

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

7.2 **Model Clauses**. To the extent that SailPoint Processes any Customer Personal Information from the EEA, the UK or Switzerland and transfers such Customer Information outside of the EEA, the UK or Switzerland to countries not deemed by the European Commission to provide an adequate level of data protection, the parties agree to enter into and comply with the Model Clauses. SailPoint agrees that it is a "data importer" and Customer is the "data exporter" under the Model Clauses (notwithstanding that the Customer may be an entity located outside of the EEA, the UK or Switzerland).

7.3 **Alternative Transfer Mechanism.** The parties agree that the data export solution identified in Section 7.2 (Model Clauses) will not apply if and to the extent that SailPoint adopts an alternative data export solution for the lawful transfer of Personal Information (as recognised under EU Data Protection Laws) outside of the EEA, the UK or Switzerland, in which event, Customer shall take any action (which may include execution of documents) strictly required to give effect to such solution and the alternative transfer mechanism will apply instead (but only to the extent such

alternative transfer mechanism extends to the territories to which Customer Personal Information is transferred).

8. Additional Security

8.1 **Confidentiality of Processing**. SailPoint shall ensure that any person who is 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).

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

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

9. Return or Deletion of Customer Personal Information

9.1 On termination or expiration of the Agreement, Customer may wish to instruct SailPoint to delete or return all Customer Personal Information (including copies) from SailPoint's systems in accordance with applicable law. SailPoint will, after a recovery period of up to 30 days following such expiry or termination, comply with this instruction as soon as reasonably practicable, where technically feasible. Customer shall be responsible for retrieving any remaining Customer Personal Information it wishes to retain before the end of the recovery period. SailPoint shall not be required to delete or return Customer Personal Information to the extent (i) SailPoint is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Personal Information; and/or (ii), Customer Personal Information it has archived on back-up systems, which Customer Personal Information SailPoint shall securely isolate and protect from any further processing, except to the extent required by applicable law.

10. Cooperation

10.1 Taking into account the nature of the Processsing, SailPoint shall (at Customer's request and expense) provide reasonable cooperation to assist Customer to respond to any requests from data subjects in relation to their data subject rights (e.g. right to access, erasure, deletion, to opt-out of sales, and any other similar data subject requests) under Data Protection Law or applicable data protection authorities relating to the Processing of Customer Personal Information under the Agreement. In the event that any request from data subjects or applicable data protection authorities is made directly to SailPoint, SailPoint shall not respond to such communication directly without Customer's prior authorisation other than to inform the requestor that SailPoint is not authorised to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to do so, and instead, after being notified by SailPoint, Customer shall respond. If SailPoint is required to respond to such a request, SailPoint will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so. For the avoidance of doubt, this Section 10.1 does not seek to diminish or exclude any right of remedy to which the data subject may be entitled pursuant to Article 82 of the GDPR.

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

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

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

11. Relationship with the Agreement

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

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

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

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

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

Annex A - Model Clauses

Standard Contractual Clauses (processors)

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

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

1. Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

2. Details of the transfer

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

3. Third-party beneficiary clause

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

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

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

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

4. Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

5. Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial

information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

6. Liability

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

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

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

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

7. Mediation and jurisdiction

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

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

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

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

8. Cooperation with supervisory authorities

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

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

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

9. Governing Law

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

10. Variation of the contract

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

11. Subprocessing

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

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

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

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

12. Obligation after the termination of personal data processing services

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

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

On behalf of the data exporter, :

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……...

On behalf of the data importer, SailPoint Technologies, Inc.:

Name (written out in full):

Position:

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

Other information necessary in order for the contract to be binding (if any): none

Signature……..

Appendix 1 to the Standard Contractual Clauses

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

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

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

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

Appendix 2 to the Standard Contractual Clauses

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

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

Please see the Security Measures, which describes the technical and organisational security measures implemented by SailPoint.

Appendix 3 to the Standard Contractual Clauses

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

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

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

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

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

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.

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

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

Clause 5(f): Audit:

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

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

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

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

3. Even where data importer cannot disclose a sub-processor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide

all information it reasonably can in connection with such sub-processing agreement to data exporter.

Clause 6: Liability

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

Clause 11: Onward sub-processing

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

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

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