Data Transfer Impact Assessment Statement
SailPoint Technologies, Inc.

At SailPoint Technologies, Inc. ("SailPoint," "we," or "us"), we take the privacy and protection of our customers' information seriously. We drafted this document to assist customers who are data exporters from the European Economic Area ("EEA"), United Kingdom, or Switzerland with completing a data transfer impact assessment pursuant to the *Schrems II* decision and the EU Standard Contractual Clauses ("SCCs"). Please note that this document does not constitute legal advice, and we recommend that you consult with your counsel regarding any intended data transfer.

What services does SailPoint provide?

SailPoint provides identity governance software solutions. SailPoint is a data processor for personal data received from or on behalf of our customers in connection with our Software-as-a-Service services ("SaaS Services"), support and maintenance services, and professional services. We enter into Data Processing Addendums ("DPAs"), including SCCs, with our customers for the processing of personal data outside the EEA, UK, and Switzerland. Our DPA terms are available at: https://www.sailpoint.com/legal/customer-agreements/.

What types of data does SailPoint process?

The types of data processed through our services include: identification and contact data (e.g., name, email 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 the customer's employees, contractors, and/or (where licensed under the Agreement) the customer's business partners and/or end-users authorised by the customer. **This type of data is typically not of interest to government or law enforcement agencies.**

SailPoint discourages and/or prohibits customers from loading sensitive personal data into our products, including special categories of personal data as referenced in Art. 9 GDPR, such as health data, political opinions, religious or philosophical

beliefs, trade union membership, race or ethnic origin, sexual orientation, genetic data, biometric data, criminal activity data, or financial account number or tax ID number.

Whose data will SailPoint process?

Our products are typically licensed for use in managing the customer's employees and contractors, in which case only employee and contractor data is processed. Again, this type of data is typically not of interest to government or law enforcement agencies.

Our customers control the types of personal data they provide to us. Our customers determine from whom the data is collected and whether this is done on an automated or voluntary basis. SailPoint will not collect personal data on the customer's behalf.

Our customer is also solely responsible for determining the legal basis for its data processing. The customer's legal basis for processing may be legitimate business interests and/or legal requirements. We would not expect customers to process employee data on the basis of consent, but the customer is responsible for that determination.

Consistent with the GDPR's "data minimization" principle, we limit the collection and transfer of data to that which is necessary in relation to the purposes for which it is processed.

Where does SailPoint process data?

For SailPoint's SaaS Services, the customer determines the location where the SaaS Services are hosted. SailPoint leverages Amazon Web Services (AWS) or Microsoft Azure for hosting its SaaS solutions. The solutions can be run from any one of several AWS/Azure Regions, based on customer proximity and preference. Although the data in the solutions will physically reside in the chosen location, the customer's SaaS Services environment will be managed, maintained, and accessed by SailPoint from its relevant locations.

A list of SailPoint's affiliates as well as third parties who may have access to personal data in connection with the SailPoint's provision of the services, as well as each of their respective locations, is available at https://www.sailpoint.com/legal/sub-processors/.

If the data will be transferred from the EEA, UK, or Switzerland to the U.S., what measures does SailPoint have in place to legitimize those data transfers?

SailPoint enters into DPAs with its customers to protect transfers of data from the EEA, UK, and/or Switzerland to the U.S. Our DPA incorporates the protections afforded by the EU SCCs. Our DPA is included in our standard terms for EMEA customers and is an option for all other customers where appropriate. Our standard contract terms are available at https://www.sailpoint.com/legal/customer-agreements/.

SailPoint has also conducted a Data Transfer Impact Assessment (DTIA) as required by the SCCs, which is summarized in this document for convenience.

SailPoint's affiliates have also entered into an Intra-group Data Transfer Agreement (IGDTA) with one another, which binds the affiliates to the SCCs in connection with their processing of personal data.

Moreover, where personal data originates from the European Economic Area and is transferred to the United States, SailPoint agrees to comply with the EU-U.S. Privacy Shield Framework and makes an affirmative commitment to adhere to EU-U.S. Privacy Shield Principles. Where personal data originates from Switzerland and is transferred to the United States, SailPoint agrees to comply with all the provisions of the U.S.-Swiss Privacy Shield Framework and makes an affirmative commitment to adhere to the U.S.-Swiss Privacy Shield Principles. SailPoint will continue to comply with these frameworks until a successor framework is available.

What controls does SailPoint have in place with sub-processors?

SailPoint will not engage a sub-processor unless we enter into a written agreement with the sub-processor imposing data protection terms that require the sub-processor to protect the customer's personal data to the same standard as SailPoint.

We also require our sub-processors to 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.

How long does SailPoint retain data?

SailPoint will only retain customer data in the SaaS Services that it processes on behalf of a customer for the duration of the SaaS Services subscription term. Data in the SaaS Services can be downloaded by the customer at any time. Within 30 days of termination or expiration of the SaaS Services, SailPoint will delete all customer data from the SaaS Services unless prohibited by law. Customer data archived on back-up systems will be securely isolated and protected from any further processing.

How is SailPoint classified?

SailPoint is classified in NAICS code 511210 for software publishers and NAICS code 518210 for hosting companies.

SailPoint is not considered a "telecommunications carrier" as defined in Section 153 of title 47 U.S.C. with respect to the services SailPoint provides to customers.

Only to the extent that SailPoint provides computer storage or processing services relating to identity governance information stored in the cloud-service by the customer, SailPoint may be considered a provider of a remote computing service.

Is SailPoint subject to FISA 702 (50 U.S.C. § 1881a)?

Section 702 of Foreign Intelligence Surveillance Act ("FISA") authorizes the U.S. government to acquire information about non-U.S. persons located outside of the U.S. through the compelled assistance of electronic communications service providers. "Electronic communications service provider" is defined broadly and encompasses telecommunication carriers, providers of electronic communications services, and remote computing services (e.g., cloud storage providers). The Department of Justice has also confirmed that other communications service providers that have access to wire or electronic communications (in transit or in storage) are included in the definition.

At least one court has construed this term as also applying to a company that provides its employees with a corporate email or a similar ability to send and receive electronic communications, regardless of the company's primary business or function. Under this broad reading, most companies—including SailPoint—would be considered electronic communications providers.

While SailPoint may provide email services to its own employees for business purposes, and thus may be considered an electronic communications service provider in that narrow context, SailPoint does not provide electronic communications services to its customers, and therefore does not meet the definition of a "provider of electronic communications service" as defined in section 2510 of title 18 U.S.C. in its services to customers.

However, SailPoint does not believe that it holds personal data that is of interest to U.S. authorities. Moreover, to date, SailPoint has never received any requests under FISA 702.

Is SailPoint subject to Executive Order 12333?

Executive Order 12333 ("EO 12333") authorizes U.S. intelligence agencies to collect foreign "signals intelligence" information (i.e. intelligence from communications and other data passed or accessible by radio, wire and other electromagnetic means). Unlike Section 702, EO 12333 does not involve compelled assistance of electronic communication service providers or create any duties or obligations for private companies. As such, we provide no assistance to, or cooperation with, the U.S. government under EO 12333.

We are not aware that the U.S. government has collected any signals intelligence from SailPoint's communications or other data. Moreover, SailPoint does not believe that it holds personal data that is of interest to U.S. authorities. We do not voluntarily disclose customers' personal data to U.S. or other government authorities, and, **in over 15 years in business, we have never been requested or compelled to provide customer data to authorities for surveillance or intelligence purposes.**

Is there a publicly available and sufficiently clear legal framework for providing U.S. public authorities access to personal data and does access satisfy necessity and proportionality restrictions?

Yes. SailPoint has assessed the applicable national surveillance laws and practices of the U.S. and has reached the following conclusions:

FISA 702 and EO 12333 do not apply to data processed by SailPoint through its SaaS Services because (1) SailPoint is a U.S. person, (2) the data is exported to a U.S. person located in the U.S., and (3) targeting of U.S. persons is prohibited.

Nevertheless, even if one presumes that U.S. public authorities were able to target data processed by SailPoint through its SaaS Services through national surveillance laws such as FISA 702, SailPoint has reviewed the four European Essential Guarantees laid out in the Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, 10 November 2020 (the "Essential Guarantee Recommendations") and has concluded that there are reasonable arguments that the laws of the U.S. are able to satisfy all four guarantees. Specifically, SailPoint has found:

A. The laws of the U.S. are based on clear, precise, and accessible rules;
B. The processing for national surveillance purposes is necessary and proportionate with regard to the legitimate objectives that are pursued by the U.S. laws;
C. U.S. laws and practices are subject to a variety of independent oversight mechanisms; and
D. There are effective remedies available to data subjects.

Based on SailPoint's review and assessment, SailPoint is able to continue transfers from the EEA, UK, and Switzerland. SailPoint will continue to evaluate its data protection commitments and strategies in light of evolving guidance.

How do we respond to government requests to access personal data of our customers?

SailPoint has not received any directive under FISA 702, National Security Letters, or other U.S. government national security request for any personal data transferred to the U.S. pursuant to SCCs. As noted in the U.S. Government's Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II* (the "US Privacy Safeguard Guidance"), "[m]ost U.S. companies do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the CJEU in *Schrems II*." This sentiment was also reflected in the U.S. Government's Comments On Proposed SCC Decisions and is particularly relevant in the context of data processed by SailPoint through its SaaS Services.

If we receive a request from a governmental authority for personal data that we process on behalf of a customer with whom we have executed a DPA, we will promptly notify the customer and, where possible, the data subject, unless we are prohibited by law from doing so. We will notify the customer about the personal data requested, the requesting authority, the legal basis for the request and the response provided. Where legally permissible, we will also notify the customer if we become aware of any direct access by public authorities to personal data that we process on behalf of the customer. If we are prohibited by law from doing so, we will use best

efforts to obtain a waiver of the prohibition with a view to communicating as much information as possible to our customer in an expeditious manner. However, as noted further above, we have not received any binding requests from any public authorities for personal data that we process on behalf of our customers.

What measures to we take to protect personal data in transit and at rest?

We have in place industry standard technical, organizational, and administrative security measures designed to protect our customers' data. Our customers also have the option of storing data collected through our SaaS Services on EEA-based servers. For additional details regarding the safeguards we employ, please refer to our security program summary at https://docs.sailpoint.com/wp-content/uploads/SailPoint-Data-Security-Program-v20210927.pdf.

What action has SailPoint taken in light of the concerns raised by the *Schrems II* judgment?

In light of *Schrems II*, SailPoint has: (i) reviewed the CJEU decision; (ii) apprised itself of currently available formal and informal guidance from the European Data Protection Board and other EEA and U.S. authorities, including the Essential Guarantee Recommendations and EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EEA level of protection of personal data, 10 November 2020, the US Privacy Safeguard Guidance, and the U.S. Government, Comments On Proposed SCC Decisions (December 10, 2020) submitted to European Commission in response to proposed SCCs; (iii) assessed the national surveillance laws in the U.S. and whether they apply to the applicable personal data transfers; (iv) reviewed the nature of the personal data it transfers to the U.S. from the EEA; (v) considered the nature, scope and number of requests it receives from the U.S. government, especially those that are of evident concern to the CJEU (i.e., involving national security surveillance); (vi) assessed whether it transfers the personal data to any additional entities and the impact that sharing has on its obligations under the SCCs; (vii) taken account of available, relevant privacy and data protection rights and redress opportunities; (viii) determined what supplementary measures it currently has in place or could implement; and (ix) re-assessed its SCCs commitments.

What additional measures has SailPoint implemented to address the concerns raised by the *Schrems II* judgment?

On an ongoing basis and in response to the *Schrems II* judgment, SailPoint will:

- Determine whether the objective facts applicable to SailPoint regarding the absence or number, or nature, of national security access requests received from the U.S. government change;
- Scrutinize government legal requests to assure that they are lawful, consistent with statutory and legally applicable criteria, are not unreasonably broad or burdensome, and do not entail requests for bulk production of personal data transferred using SCCs;
- Continue to assess, on an ongoing basis, the access requests it receives to determine whether it can sustain a good faith view that the requests it receives are valid, not disproportionate and subject to appropriate safeguards consistent with the presidential directive that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information;
- Review applicable laws, oversight mechanisms, relevant guidance and other relevant developments in the United States and EEA/UK as it develops to consider the impact of the legal regime on SailPoint's data protection obligations under its SCCs;
- Consult with SailPoint's data exporting entities in the EEA/UK regarding compliance with its contractual data transfer obligations if and when SailPoint's self-assessment should suggest that factors identified by the CJEU in *Schrems II* could block SailPoint's obligation to accord privacy and data protection rights to EEA/UK persons as contemplated in *Schrems II*;
- Review and amend SailPoint's SCCs in accordance with future guidance or updated model contractual provisions issued by EEA authorities;
- Take such other actions as deemed necessary or appropriate to comply with the privacy, data protection and data transfer provisions of the GDPR;

- Use industry-standard strong encryption methods to protect data in transit and at rest, in each case as appropriate to the sensitivity of the data and the risks associated with loss;
- Encrypt all laptops and other removable media (including backup tapes) on which customer personal data is stored;
- Maintain authorization controls to limit access of personal data to authorized personnel;
- Use industry-standard measures to detect and remediate malware, viruses, ransomware, spyware and other intentionally harmful programs that may be used to gain unauthorized access to information or systems;
- Maintain a policy and process in place to deal with instances where a data subject wishes to exercise their GDPR data privacy rights (e.g., right to erasure, rectification or access etc.); and
- Implement all necessary policies and procedures to deal with (and, to the extent possible and appropriate, object to) any U.S. or other third party government access requests for personal data processed by SailPoint.

SailPoint's answers to common "yes/no" *Schrems II* questions:

1 Direct Application of 50 U.S.C. § 1881a (FISA 702)

1.1 Do you or any other relevant U.S. entity (controller or processor) that processes or has access to personal data that is transferred to you fall under any of the following definitions in 50 U.S.C.§ 1881(b)(4) that could render you or the other entity(ies) directly subject to 50 U.S.C. § 1881a (FISA 702)?

X Yes □ No □ We are under a legal obligation not to answer this question

1.2 Especially, do you or any other entity located in the U.S. which processes or has access to personal data that [Customer] transferred to you

(A) qualify as a telecommunications carrier, as that term is defined in section 153 of title 47 U.S.C.?

□ Yes **X No** □ We are under a legal obligation not to answer this question

(B) qualify as a provider of electronic communication service, as that term is defined in section 2510 of title 18 U.S.C.?
□ Yes **X No** □ We are under a legal obligation not to answer this question

(C) qualify as a provider of a remote computing service, as that term is defined in section 2711 of title 18 U.S.C.?
X Yes □ No □ We are under a legal obligation not to answer this question

(D) qualify as any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored?
□ Yes **X No** □ We are under a legal obligation not to answer this question

(E) qualify as an officer, employee, or agent of an entity described in (A), (B), (C), or (D)?
X Yes □ No □ We are under a legal obligation not to answer this question

2 Indirect Enforcement of FISA 702

2.1 Are you controlled by a U.S. parent company or shareholder, or do you have another relevant tie to the U.S. that could make U.S. law indirectly enforceable against you?
□ Yes **X No** □We are under a legal obligation not to answer this question
SailPoint is directly subject to U.S. law.

2.2 If so, are you, as a matter of EU law, national law, corporate or private international law, required to ignore any order, request or directive from a U.S. entity that would require you to expose any of the personal data that

you process to the U.S. government under 50 U.S.C. § 1881a (= FSIA 702) or EO 12.333 and are you in fact able to block such access?

□Yes □ No □We are under a legal obligation not to answer this question

Please specify what legal and/or technical protections you rely on:

N/A

3 Processing under EO 12333

Do you, or any other relevant U.S. entity (controller or processor) that processes personal data that is transferred from us to you, cooperate in any respect with U.S. authorities conducting surveillance of communications under EO 12333, irrespective of whether such cooperation is mandatory or voluntary?

□ Yes **X No** □We are under a legal obligation not to answer this question

SailPoint does not cooperate directly and has no knowledge of whether any other relevant U.S. entity may be cooperating, with surveillance of communications under EO 12333.

4 Other relevant Laws

Are you or any other relevant U.S. entity (controller or processor) that processes personal data that is transferred from us to you subject to any other law that could be seen as undermining the protection of personal data under the GDPR (Article 44 GDPR) or under Swiss law?

□ Yes **X No** □We are under a legal obligation not to answer this question

5 Measures against Mass and Indiscriminate Processing in Transit (FISA 702 and EO 12333)

As the Court of Justice has also highlighted the need to ensure that personal data is not subject to mass surveillance in transit, we seek the following clarifications:

A. Have you implemented appropriate technical and organisational measures (see Article 32 GDPR) for every step of the processing operations which ensure that mass and indiscriminate processing of

personal data by or on behalf of authorities in transit (such as under the "Upstream" program in the U.S.) is made impossible?
X Yes □ No □ We are under a legal obligation not to answer this question

B. If you have answered 'yes' to the previous question, please specify which technical and organisational measures (including encryption) have been taken so that neither content nor metadata can be processed by sophisticated state actors with direct access to the internet backbone, switches, hubs, cables and alike:
Please see the following website for SailPoint's security terms and approach: https://docs.sailpoint.com/wp-content/uploads/SailPoint-Data-Security-Program-v20210927.pdf.

Does SailPoint have a Data Protection Officer?

Yes. SailPoint has appointed a Data Protection Officer who can be reached at privacy@sailpoint.com.