SAILPOINT JOB APPLICANT PRIVACY NOTICE

Effective Date: September 29, 2023

SailPoint Technologies, Inc. and its operating groups, subsidiaries and affiliates, (the "Company," "us" or "we") are committed to protecting the privacy and security of the personal information you provide to us. Please read this Job Applicant Privacy Notice (the "Privacy Notice") to learn how we treat your personal information when you apply for a job or other role with us. If you are one of our job applicants located in the European Economic Area ("EEA"), Switzerland, and the United Kingdom ("UK"), or California, you have certain rights under the General Data Protection Regulation and as the General Data Protection Regulation EU GDPR forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (collectively, together, the "GDPR") or California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CCPA"), respectively, with respect to your personal information, as outlined below. In this Privacy Notice, the term "personal data" has the meaning set forth under the CCPA and includes the definition of "personal data" as defined under the GDPR. This Privacy Notice only applies to job applicants who are residents of the State of California or individuals located in the EEA, Switzerland, and the UK.

As we continually work to improve our operations and business, we may need to change this Privacy Notice from time to time. Upon material changes, we will alert you to any such changes by placing a notice on the Company's intranet, by sending you an email and/or by some other means.

Privacy Notice Table of Contents

1 What Categories of Personal Information Do We Collect?

This chart details the categories of personal information that we collect and have collected over the past twelve (12) months:

Category of Personal Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
Identifiers	• Real name • Alias • Postal address • Unique personal identifier (including, telephone number or device identifier) or online identifier • IP address • Email address • Account name • Social security number • Driver's license number or passport number • Other similar identifiers	• Service Providers • Affiliates
Categories of Personal Information Described in California Customer Records Act (Cal. Civ. Code § 1798.80(e))	• Name • Signature • Social security number • Physical characteristics or description • Address • Telephone number • Passport number, driver's license or state identification card number • Insurance policy number	• Service Providers • Affiliates

Category of Personal Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
	• Educational information • Employment or employment history • Bank account number or any other financial information • Medical information or health insurance information	
Characteristics of Protected Classifications under California or Federal Law	• Race • Religious creed • National origin • Ancestry • Physical or mental disability • Medical condition • Marital status • Sex, gender, gender identity, or gender expression • Age • Military and veteran status	• Service Providers • Affiliates
Internet or Other Electronic Network Activity Information	• Information regarding your interaction with an internet website, application, or advertisement (including chats, instant messaging, account user names and user roles) • Browser Type • Operating System Type	• Service Providers • Affiliates
Geolocation Data	• IP-address-based location information	• Service Providers • Affiliates
Photos, Videos, or Recordings	• Photos, or videos of you • Photos, or videos of your environment	• Service Providers • Affiliates

Category of Personal Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
Professional or Employment-Related Data	• Resume • Job title • Job history • Performance evaluations • Union membership • Information provided to us or created by us as part of your job application, such as interview notes, responses to screening questions and assessment results • Signature	• Service Providers • Affiliates
Education Information (as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99))	• Grades or transcripts • Student financial information • Student disciplinary records	• Service Providers • Affiliates
Categories of Personal Information Considered "Sensitive" Under the California Privacy Rights Act	• Social security, driver's license, state identification card or passport numbers • Account log-in, financial account, in combination with any required security or access code, password or credentials allowing access to an account • Racial or ethnic origin • Religious beliefs • Contents of your mail, email, and text messages where the Company is not the intended recipient of the communication	• Service Providers • Affiliates

2 Categories of Sources of Personal Information

We collect personal information from the following categories of sources:

- You
  - When you provide such information directly to us.
- Public Records
  - From the government or other sources.
- Third Parties. For example, we may collect information from:
  - Vendors
    - Recruiters.
    - Pre-employment screening services.
    - Credentialing and licensing organizations.
    - Consumer reporting agencies.
  - Prior employers (e.g., for references)
  - Professional references
  - Educational institutions
  - Publicly Available Sources
    - Social networks, including your social media profile (e.g., LinkedIn, Twitter and Facebook).
    - Other sources you identify or refer us to.

3 Our Commercial or Business Purposes for Collecting or Disclosing Personal Information

- Recruiting and/or Hiring You and Operating, Hosting and Facilitating Our Operations and Business
  - Processing and managing your application.
  - Conducting background and reference checks.
  - Providing immigration support.
  - Entering into contracts.
  - Implementing, managing and improving the Company's recruitment process and diversity and inclusion programs.
  - Implementing health and safety measures and maintaining a safe workplace.
  - Managing the Company's relationship with you.

    - Meeting or fulfilling the reason you provided the information to us.
    - Maintaining the security of our systems and property, and doing fraud protection, security and debugging.
    - Carrying out other business or employment-related purposes stated when collecting your personal information or as otherwise set forth in applicable data privacy laws, such as the CCPA or the GDPR.

- Meeting Legal Requirements and Enforcing Legal Terms
    - Fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting and investigating security incidents and potentially illegal or prohibited activities, or responding to lawful requests by public authorities, including to meet national security or law enforcement requirements.
    - Protecting the rights, property or safety of you, the Company or another party.
    - Enforcing any agreements with you.
    - Responding to claims.
    - Resolving disputes.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated or incompatible purposes without providing you notice.

4 How We Share Personal Information

We disclose your personal information to the categories of service providers and other parties listed in this section.

- Affiliates. Our affiliates help us to perform business functions on our behalf.
- Service Providers. These parties help us to perform business functions on our behalf. They include:
    - Hosting, technology and communication providers.
    - Security and fraud prevention consultants.
    - Background and reference check screening services.
    - Hiring process management and administration tools.

Legal Obligations

We may share any personal information that we collect with third parties in conjunction with any of the activities set forth under "Meeting Legal Requirements and Enforcing Legal Terms" in the "Our Commercial or Business Purposes for Collecting or Disclosing Personal Information" section above.

Business Transfers

All of your personal information that we collect may be transferred to a third party if we undergo a merger, acquisition, bankruptcy or other transaction in which that third party assumes control of our business (in whole or in part). Should one of these events occur, we will make reasonable efforts to notify you before your information becomes subject to different privacy and security policies and practices.

Information that is Not Personal Information

We may create aggregated, de-identified or anonymized data from the personal information we collect, including by removing information that makes the data personally identifiable to a particular job applicant. We may use such aggregated, de-identified or anonymized data and share it with third parties for our lawful business purposes, including to operate, host and facilitate our operations and business, provided that we will not share such data in a manner that could identify you.

5 Data Security

We seek to protect your personal information from unauthorized access, use and disclosure using appropriate physical, technical, organizational and administrative security measures based on the type of personal information and how we are processing that information. You should also help protect your data by appropriately selecting and protecting your password and/or other sign-on mechanism, limiting access to your computer or device and browser, and signing off after you have finished accessing your account. Although we work to protect the security of your account and other data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure.

6 Data Retention

We retain personal information about you for as long as necessary to perform our business or commercial purposes, including employment-related purposes, for collecting your personal information. When establishing a retention period for specific categories of personal information, we consider who we collected the personal information from, our need for the personal information, why we collected the personal information, and the sensitivity of the personal information. In some cases we retain personal information for longer, if doing so is necessary to comply with our legal obligations, resolve disputes or collect fees owed, or is otherwise permitted or required by applicable law, rule or regulation. We may further retain information in an anonymous or aggregated form where that information would not identify you personally.

7 Job Applicant Rights under the GDPR

If you are a job applicant located in the EEA, Switzerland, or the UK, we are required to provide you with additional information about our processing of your personal information. Please note that, except as otherwise provided by applicable law, the information in this section as well as the other sections of this Privacy Notice apply to you.

If you are a job applicant located in the UK, Switzerland or EEA, the Company is the controller of your personal information. As a data controller, the Company is responsible for ensuring that the Company's processing of your personal information complies with the GDPR.

Processing of Sensitive Personal information

We may collect and process certain sensitive personal information about you, such as your racial or ethnic origin or data concerning your health to the extent such processing is necessary for us to carry out our obligations with respect to your employment or benefits provided to you as a result of your employment.

Legal Basis for Processing your Personal Information

We only process your personal information where applicable law permits or requires it, including where the processing is necessary to assess your potential employment with us, where the processing is necessary to comply with our legal obligations or for our legitimate interests or the legitimate interests of third parties, or with your consent. We may process your personal information for legitimate business purposes and for the following purposes:

- **Process and manage your application:** We use your personal information to process your job application, establish a job applicant profile for the recruitment process, assess your qualifications for a specific role with us, schedule and conduct interviews, communicate with you, and carry out background and reference checks (see the following bullet point for additional information). We may collect audio and visual information of job applicants through photographs used for identification purposes. With your consent, we may record video of you in connection with the application process, for example through a third party screening service. Additionally, if you are offered a position with us, we may use your personal information in the employee on-boarding process.
- **Conduct reference and background checks (as permitted by applicable law):** We use personal information we collect to conduct reference checks and to evaluate your qualifications and experience. We may also conduct background checks (as authorized by you and permitted by applicable law).
- **Provide immigration support:** If applicable and as permitted by applicable law, we may collect your personal information to assist with immigration support, such as applying for visas or work permits.
- **Analyze and improve our recruitment process and tools**: For example, we analyze trends in our applicant pool, and use personal information to understand and improve our recruitment process and tools (including improving diversity and inclusion).
- **Record-keeping:** We keep records of your personal information as required by law and in accordance with our record retention policies.
- **Meeting legal requirements and enforcing legal terms:** We collect and process your personal information for purposes of: fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting and investigating security incidents and potentially illegal

or prohibited activities; protecting the rights, property or safety of you, us or another party; enforcing any agreements with you; responding to claims; and resolving disputes. Additionally, we may use information about protected characteristics to analyze and monitor the diversity of our job applicants in accordance with applicable laws.

We will only process your personal information for the purposes we collected it for or for compatible purposes. If we need to process your personal information for an incompatible purpose, we will provide notice to you and, if required by law, seek your consent. We may process your personal information without your knowledge or consent where required by applicable law or regulation.

We may also process your personal information for our own legitimate interests, including for the following purposes:

- To prevent fraud.
- To ensure network and information security, including preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution.
- To support internal administration with our affiliated entities.
- To conduct data analytics analyses to review and better understand our recruitment process.

You will not be subject to decisions based on automated data processing without your prior consent.

Rights of Access, Correction, Erasure, and Objection

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during the recruitment process. By law, you may have the right to request access to, correct, and erase the personal information that we hold about you, or object to the processing of your personal information under certain circumstances. You may also have the right to request that we transfer your personal information to another party.

Right to Withdraw Consent

Where you have provided your consent to the collection, processing, or transfer of your personal information, you may have the legal right to withdraw your consent under certain circumstances.

We may request specific information from you to help us confirm your identity and your right to access, and to provide you with the personal information that we hold about you or make your requested changes. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal information that we hold about you, or we may have destroyed, erased, or anonymized your personal information in accordance with our record retention obligations and practices. If we cannot provide you with access to your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Cross-Border Data Transfers

Where permitted by applicable law, we may transfer the personal information we collect about you to the United States and other jurisdictions that may not be deemed to provide the same level of data protection as your home country for the purposes set out in this Privacy Notice. Where necessary, we have implemented standard contractual clauses to help secure the transfer and/or rely on the Data Privacy Framework, as described below.

Additionally, SailPoint and our affiliates, SailPoint International, Inc. and SailPoint Technologies Holdings, Inc. comply with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF ("UK-U.S. DPF"), and the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF") (collectively, the "DPF") as set forth by the U.S. Department of Commerce. SailPoint has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("EU-U.S. DPF Principles") with regard to the processing of all personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF (the "EU-UK DPF Principles"). SailPoint has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles ("Swiss-U.S. DPF Principles") with regard to the processing of personal data received from Switzerland in reliance on the

Swiss-U.S. DPF (the EU-U.S. DPF Principles, the EU-UK DPF Principles, and the Swiss-U.S. DPF Princples, collectively, the "DPF Principles"). If there is any conflict between the terms in this Privacy Notice and the DPF Principles, the DPF Principles shall govern. To learn more about the DPF, and to view our certification, please visit https://www.dataprivacyframework.gov/.

The Federal Trade Commission has jurisdiction over SailPoint's compliance with the DPF. This Privacy Notice describes the types of Personal Data we collect, the purposes for which we collect and use your Personal Data, and the purposes for which we disclose your Personal Data to certain types of third parties in the sections above. Pursuant to the DPF, EU, UK, and Swiss individuals have the right to obtain our confirmation of whether we maintain Personal Data relating to you in the U.S. Upon request, we will provide you with access to the Personal Data that we hold about you. You may also correct, amend, or delete the Personal Data we hold about you. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the U.S. under DPF, should direct their query to privacy@sailpoint.com. If requested to remove data, we will respond within a reasonable timeframe.

In addition, we will provide you with the choice to opt-out from the sharing of your Personal Data with any third parties (other than our agents or those that act on our behalf or under our instruction), or before we use it for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized.

We will provide you with the choice to opt-in to sharing your sensitive Personal Data with any third parties or if we plan to process your Personal Data for a purpose other than those for which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your Personal Data, please submit a written request to privacy@sailpoint.com.

In addition to any other disclosures described in this Privacy Notice, in certain situations, we may be required to disclose Personal Data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

SailPoint's accountability for Personal Data that it receives in the U.S. under the DPF and subsequently transfers to a third party acting as an agent on our behalf is described in the DPF Principles. In particular, SailPoint remains liable under the DPF Principles if our agents process Personal Data in a manner inconsistent with the DPF Principles, unless SailPoint proves that we are not responsible for the event giving rise to the damage.

In compliance with the DPF, SailPoint commits to resolve DPF Principles-related complaints about our collection and use of your Personal Data. EU, UK, and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the DPF should first contact SailPoint at privacy@sailpoint.com.

Further, SailPoint commits to cooperate and comply with, respectively, the panel established by the EU data protection authorities and the Swiss Federal Data Protection and Information Commissioner with regard to unresolved complaints concerning our handling of human resources data received in reliance on the DPF in the context of the employment relationship.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Annex 1 of the DPF Principles, located at https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2.

8 Job Applicant Rights under the CCPA

You have the rights set forth in this section. Please see the "Exercising Your Rights" section below for instructions regarding how to exercise these rights. Please note that these rights may be subject to certain requirements, restrictions, and exceptions under the CCPA, which may permit or require us to deny your request.

Access

You have the right to request certain information about our collection and use of your personal information over the past twelve (12) months. In response, we will provide you with the following information:

- The categories of personal information that we have collected about you.
- The categories of sources from which that personal information was collected.
- The business or commercial purpose for collecting or selling your personal information.
- The categories of third parties with whom we have shared your personal information.
- The specific pieces of personal information that we have collected about you.

If we have disclosed your personal information to any third parties for a business purpose over the past twelve (12) months, we will identify the categories of personal information shared with each category of third party recipient. If we have sold your personal information over the past twelve (12) months, we will identify the categories of personal information sold to each category of third party recipient.

Deletion

You have the right to request that we delete the personal information that we have collected about you. Under the CCPA, this right is subject to certain exceptions: for example, we may need to retain your personal information if deletion of your personal information involves disproportionate effort. If your deletion request is subject to one of these exceptions, we may deny your deletion request.

Correction

You have the right to request that we correct any inaccurate personal information we have collected about you. Under the CCPA, this right is subject to certain exceptions: for example, if we decide, based on the totality of circumstances related to your personal information, that such data is correct. If your correction request is subject to one of these exceptions, we may deny your request.

Processing of Sensitive Personal Information Opt-Out

We collect personal information that is considered "sensitive personal information" under the CCPA. Consumers have certain rights over the processing of their sensitive personal information. Please note that we only use or disclose your sensitive personal information for the purposes set forth in section 7027(m) of the CCPA regulations and we do not collect or process sensitive personal information with the purpose of inferring any characteristics about California residents.

Personal Information Sales Opt-Out and Opt-In

We will not sell your personal information, and have not done so over the last twelve (12) months. To our knowledge, we do not sell the personal information of minors under sixteen (16) years of age.

Personal Information Sharing Opt-Out and Opt-In

Under the CCPA, you have certain rights when a business "shares" personal information with third parties for purposes of cross-contextual behavioral advertising. We will not share your personal information for cross-contextual behavioral advertising, and have not done so over the last twelve (12) months. To our knowledge, we do not share the personal information of minors under sixteen (16) years of age for purposes of cross-contextual behavioral advertising.

We Will Not Discriminate Against You for Exercising Your Rights Under the CCPA

We will not discriminate against you for exercising your rights under the CCPA. Job applicants will not be subject to any retaliation or disciplinary action for exercising their rights under the CCPA.

9 Exercising Your Rights

To exercise the rights described in this Privacy Notice, you or your Authorized Agent (defined below) must send us a request that (1) provides sufficient information to allow us to verify that you are the person about whom we have collected personal information, and (2) describes your request in sufficient detail to allow us to understand, evaluate and respond to it. Each request that meets both of these criteria will be considered a "Valid Request." We may not respond to requests that do not meet

these criteria. We will only use personal information provided in a Valid Request to verify your identity and complete your request. You do not need an account to submit a Valid Request.

We will work to respond to your Valid Request within the time period required by applicable law. We will not charge you a fee for making a Valid Request unless your Valid Request(s) is excessive, repetitive or manifestly unfounded. If we determine that your Valid Request warrants a fee, we will notify you of the fee and explain that decision before completing your request.

You may submit a Valid Request using the following methods:

- Filling out a request at the following link
- Write us at:
  SailPoint Technologies, Inc.
  c/o Privacy Team
  11120 Four Points Dr., Suite 100
  Austin, Texas 78726
- For California residents, calling us at: 1-877-378-1220

You may also authorize an agent (an "Authorized Agent") to exercise your rights on your behalf. To do this, you must provide your Authorized Agent with written permission to exercise your rights on your behalf, and we may request a copy of this written permission from your Authorized Agent when they make a request on your behalf.

10 Contact for Questions

If you have any questions or comments regarding this Privacy Notice, the ways in which we collect and use your personal information or your choices and rights regarding such collection and use, please contact:

- privacy@sailpoint.com
- SailPoint Technologies, Inc.
  c/o Privacy Team
  11120 Four Points Dr., Suite 100
  Austin, Texas 78726

To make any accessibility-related requests or report barriers, please contact us at 512-346-2000 or contact us at HR@sailpoint.com.