splunk> turn data into doing

SPLUNK RECRUITING & COMMUNITY INTERACTION PRIVACY NOTICE

Updated: May 2023

Splunk Inc. and its subsidiaries (collectively, "Splunk", "we" or "us") are committed to safeguarding your Personal Information and privacy rights. This Recruiting and Community Interaction Privacy Notice ("Privacy Notice") explains how we collect, use, store and share your information when you apply for a position at Splunk as a job applicant or internal contractor, potential candidate for employment at Splunk or for a contractor position Splunk offers, internship, or scholarship, or to participate in our recruiting or skill improvement programs and events ("Information"). Information includes Personal Information, by which we mean Information about an identified or reasonably identifiable individual.

Applications for positions globally are managed by Splunk through the Careers at Splunk website hosted in the U.S.

For information about how Splunk collects, uses, and discloses other types of information, e.g. via the Splunk website, please refer to the general Splunk Privacy Policy.

Information We Collect

Throughout the application process at Splunk we collect Information from you. Some Information is required to process your application, other Information is optional only. Below is a list of the types of Information we collect, noting those which are optional or permitted only in certain locations.

Identifiers, such as:

- Name
- Phone number(s)
- Email address
- Home address
- Other information you make available, such as a URL or handle for a social media or open-source platform (optional)

Education information, such as:

- School/training history included in your resume/CV, transcripts, cover letter, or otherwise supplied in an interview
- Schools attended

- Graduation date(s)
- Degrees/certifications received or in progress
- Descriptions of technical capabilities where relevant (e.g., proficient in JAVA)

Professional or employment-related information, such as:
- Employment history
- Compensation expectations
- LinkedIn or Facebook profile and related URL (optional)
- Past and current job titles
- Identification numbers associated with professional credentials and certifications
- Questions that help Splunk identify or determine:
    - your legal right to work in the country in which you are applying (including visa status)
    - whether you are open to relocation
    - how you learned about the position
    - relevant criminal history (where permitted)
    - any non-compete or non-solicitation obligations that you may have which could prevent or curtail your ability to perform the role for Splunk to which you have applied
    - any actual or potential conflicts of interest
- Relevant skills
- Past performance and achievements

Characteristics of protected classes, such as:
- Gender (optional)
- Race / ethnicity (U.S. positions only, optional)
- Veteran status (U.S. positions only, optional)
- Citizenship or residency (U.S. and Singapore positions, as required by law)
- Disability status (U.S. positions only, optional)
- Medical history (only in locations where an exam is required as a condition of employment)
- Age (inferred from birthdate when used for pre-employment screening checks as described below)

Internet or other electronic network activity information, as permitted by law.
- Data collected by cookies from website visits, such as frequency and duration of visits as further described in the Splunk Cookie Policy. (Optional)

Information that is “optional” is provided voluntarily by you, and no adverse action or decision will be made against you if you choose not to provide any optional information.

As you progress through the process additional information may be requested or required. We, or a third party on our behalf, may also collect sensitive information (e.g., in some countries health exam information) where required by applicable law and with your consent (when required). Your consent may be withdrawn at any time by contacting us as described in Contact Us. Please note that if you do not consent or withdraw your consent we may not be able to fully assess your application.

Much of the Information we collect is obtained from you (e.g. during interviews or via assessments), but we also obtain some Information about you in the process, from third parties, including, for example, recruiters, your references, prior employers, and companies that perform pre-employment checks, or online sources. We may also collect publicly available Information about you online, such as your profile on a professional social media website.

Applying for a Position, Scholarship, or to Participate in Splunk Programs

When we receive your application, you usually receive a system-generated email confirming receipt.

If you are applying for a position, scholarship, or program in one of our offices or locations outside the U.S., we will pass along your Information to the relevant local subsidiary, office, and recruitment team(s) so that they can consider your application.

For certain job openings or programs in the U.S., you may receive a form from Splunk (via its third-party recruiting systems) with optional questions asking for additional Personal Information, such as your gender, ethnicity, race, disability, and veteran status. Your responses are aggregated and included in an affirmative action plan along with accompanying reports that we are required to complete by the U.S. Office of Federal Contractor Compliance Programs (OFCCP) in our capacity as a U.S. federal government contractor. Splunk does not consider this Information in the hiring process.

Upon receipt of your application, we will review your credentials, Information, and the requirements of the position, scholarship, or program. If we find there is a potential match, we may follow up with you.

Pre-employment Screening Checks

At various points in the application, interview, and hiring process, you may be subject to pre-employment screening, as permitted by applicable law. The type of screening we perform and the Information we collect as a result will depend upon the role for which you have applied, as well as the country in which you would work if ultimately hired.

The objectives of the pre-employment screening are to validate and collect Information about:

- Education history
- Past employment history (including dates of employment and positions held)
- Criminal background (if/as permitted)
- Credit status (if/as permitted and based on position)
- Professional licence verification (as permitted and based on position)

Splunk relies on third parties to conduct pre-employment screenings and we will release your Information to them for this purpose, with your prior consent as required by law. We, or third parties on our behalf, will supply you with information about the nature and scope of the screening and obtain your prior consent, including your consent to the release of any required documents. Your consent may be withdrawn at any time. If, due to not granted or withdrawn consent, we cannot perform the pre-employment screening, we may not be able to fully assess your application and may be unable to hire you.

Disclosing Information

We may disclose your Information to our subsidiaries, or with third parties that provide services to us, such as those assisting with the application, interview, and/or hiring process (e.g., external recruiters or vendors that perform pre-employment checks).

If you have been referred by a current Splunk employee, we may inform that employee about the progress of your application and let the employee know the outcome of the process. For referrals, it is the referring employee's responsibility to obtain prior consent to share the applicant's Personal Information with Splunk as part of the application process.

We may transfer your Information to your references, your current or former employer or organization, or subsidiaries or affiliates under common ownership or control of Splunk. Your Information may be disclosed to relevant third parties in connection with any proposed or actual reorganization, sale, merger, consolidation, joint venture, assignment, transfer, or other disposition of all or part of our business, assets, or stock (including in connection with any bankruptcy or similar proceeding).

Information may be disclosed to third parties to comply with legal reporting obligations, such as those associated with equal employment and affirmative action programs, to detect, prevent, or otherwise

address fraud, security or technical issues, or to protect against harm to the rights, property or safety of Splunk, applicants, candidates, employees, or the public, or as otherwise legally permitted.

Using Information

Your Information will be held in our electronic systems or manually in our files and used by us to evaluate your application and qualifications and to contact you during the process. For those that apply, if your application is successful, we will use your Information to make an offer of employment, internship, scholarship, or join a program. We may also use your Information to consider you for other opportunities at Splunk for which you may also be qualified (unless you specifically request in writing that you do not want us to do so), to meet recordkeeping requirements and reporting responsibilities, in investigations, or as needed in legal proceedings.

We may retain your Information as described below in Records Retention. We may also use certain "optional" Information to create anonymous, aggregated statistics in support of programs such as gender or race/ethnic equity and diversity programs, and "optional" Information such as disability status to determine working conditions or necessary accommodations. We may use your Information for analytics purposes, including in aggregated or pseudonymized form (from which your name, contact details and other elements that directly identify you are removed), to improve our recruiting and hiring process. We may use your Information to protect the rights and property of Splunk, our applicants, candidates, employees, or the public as required or permitted by law.

Our processing of your Personal Information for the purposes mentioned above is based on our legitimate business interests, our performance of contractual and precontractual measures relating to our potential relationship with you, our compliance with applicable law, or your consent.

Automated Tools

We may perform searches against our applicant database or other sources using automated tools to target relevant job requirements and match them against your credentials. You may be asked to successfully complete assessments that are relevant to the role, and such assessments may make use of automated tools. However, we do not make hiring decisions based solely on automated processes.

Security

Splunk takes reasonable technical and organizational measures to safeguard Personal Information against loss, theft, and unauthorized access, disclosure, alteration, misuse, or destruction. Unfortunately, no data transmission, software, or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of an account has been compromised), please notify us immediately in accordance with the Contact Us section below. If Splunk learns of a breach of its systems, we may notify you or others consistent with applicable law and/or as agreed in our contract with you if applicable. Splunk may communicate with you electronically regarding privacy and security issues affecting Information collected through the application process.

Records Retention

If your application is successful, we will put some of your recruitment Information in your employment, scholarship, or program files. We will only include Information that is relevant to your ongoing relationship with Splunk and to perform analytics (in aggregated or pseudonymized form as described above) to improve our processes. Once your relationship with Splunk begins, how we handle your Information is governed by our Data Protection Policies, the Employee Data Protection Notice, other specific internal notices, as well as your contract or offer letter, as applicable. This Information will be

retained for the life of your relationship with Splunk and for additional time thereafter. For details, see the Record Retention Schedule after joining Splunk.

If your application is unsuccessful or you withdraw from the process or decline an offer, application forms and related documentation will be kept on file for as long as needed to comply with any legal or document retention obligations, or in case we face a legal challenge with respect to a decision.

After your recruitment records are no longer needed, we will dispose of them in a secure manner in accordance with applicable law. Unless we face a legal challenge with respect to a hiring decision, these records will be disposed of after 24 months (EEA, UK and Switzerland) or after four years (US and other countries outside of the EEA/UK/Switzerland.

Cross-border Transfers

Your Personal Information may be stored and processed in any country where we have facilities or in which we engage service providers. By applying to a position, for a scholarship, or to participate in a program at Splunk, you acknowledge that we may transfer and process your Personal Information outside of your country of residence, including to the United States, where different data protection laws may apply.

Splunk has entered into standard contractual clauses for relevant transfers of Personal Information within the Splunk group of companies, and with service providers with whom we share your Personal Information. You can obtain a copy by contacting DPO@Splunk.com.

Splunk has certified to the U.S. Department of Commerce that we adhere to the Privacy Shield Principles of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks, as further described in the Splunk Privacy Shield Notice. Splunk does not currently rely on the frameworks as a legal basis for transfers of Personal Information from the EEA, Switzerland or the UK. If there is any conflict between the terms in this Privacy Notice and the Privacy Shield Principles, the Principles will govern. To learn more about the Privacy Shield program, please visit privacyshield.gov, where you can view Splunk's certifications.

Pursuant to our Privacy Shield certification, complaints regarding the enforcement of this Privacy Notice may be addressed to us at privacyshield@splunk.com or via JAMS, a U.S.-based independent dispute-resolution body. If neither Splunk nor JAMS can resolve your complaint, you have the right to invoke binding arbitration. You may also have a right to lodge a complaint with your local data protection authority.

If you have any questions or require more information about cross-border transfers of Personal Information, please see Contact Us below.

Your Rights

In certain locations, you may have rights under data protection law, such as to request:

- what Personal Information has been collected and transferred
- access to or correction of your Personal Information ,
- deletion of your Personal Information ,
- transfer of your Personal Information , or
- to object to or restrict Splunk from using Personal Information for certain purposes.

If you would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Information at issue, through our data request form, and we will respond as soon as reasonably practicable consistent with applicable law. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

Supplemental Terms and Conditions for Certain Regions

European Economic Area, the UK, and Switzerland

If you have any questions or concerns about Splunk's privacy practices, you can contact us at any time via the contact options listed under Contact Splunk below. If your request or concern is not satisfactorily resolved by us, you can approach your local data protection authority. You can find your local data protection authority in the EU here and in the UK here.

US State Laws

California

For purposes of California law, "Personal Information" means Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a consumer or household.

California law provides you with specific rights in addition to those listed in the "Your Rights" section above regarding your "Personal Information" subject to certain exceptions. Those additional rights include:

- the right to request disclosure of Personal Information sold or shared;
- the right to opt-out of the sale of sharing of Personal Information; and
- the right to non-discrimination for exercising your rights

In addition to exercising your rights on the form linked above, you may call our toll-free number 1-888-914-9661 PIN #: 587261 and we will respond in accordance with our legal obligations. We will verify your identity, and the identity of any third-party agent acting on your behalf, before we comply with the request and ask for your cooperation with our identity verification process. Please note that we are only required to respond to two such requests per individual each year.

Splunk does not sell or share your Personal Information as defined by California law.

Contact Us

If you have any questions about this Privacy Notice, including about how Splunk collects, uses, transfers, or discloses the Personal Information you provide, please contact our Data Protection Officer at DPO@splunk.com or by writing to us at any of the addresses below:

Splunk Inc. Office of the Data Protection Officer 270 Brannan Street San Francisco, CA 94107	Splunk Services UK Limited Office of the Data Protection Officer Brunel Building 1 & 2 Canalside Walk London W2 1DG England	Splunk Services Germany GmbH Office of the Data Protection Officer Mies-van-der-Rohe-Straße 6 80807 München Germany

Please note that email communications are not always secure, so please do not include sensitive information in your emails to us.

We may change this Privacy Notice from time to time and will post our updates here.