VMware Applicant Privacy Notice

Effective Date: January 1, 2023

VMware, Inc., headquartered in the U.S., and its group companies (“VMware”, “we”, “us” and “our”) are committed to protecting your privacy. This Applicant Privacy Notice ("Applicant Notice") describes the privacy practices that applies to our collection, use and disclosure of personal information about candidates (“applicant”, "you" and "your") in connection with the recruitment and application processes for employment, contingent work, scholarship and/or internship opportunities with us when you submit personal information to us via any of our application portals or other recruitment mediums, whether online or off-line (collectively, the "Sites"), as well as how we use and share that information. See our VMware Global Privacy Notice to learn about our privacy practices that apply to other interactions with us, such as when you visit our website to learn about our services. We appreciate your interest in VMware and take care to process and use your information responsibly.

PART I: What Information We Collect & How We Collect It

What information we collect

- Personal information. We collect and process personal information in connection with your candidacy, including educational, work, and employment background, contact information and preferences, job qualifications, references and jobs or other career opportunities for which you would like to submit an application. You also may choose to provide us with additional information, such as your CV, resume, or transcripts; employment and work references and related information; and compensation requests.

- Sensitive personal information. We may also collect certain types of personal information that is treated as sensitive personal information. Often sensitive information is voluntarily shared by you, and not required or requested by us. Sensitive personal information includes, for example, government-issued identification number (such as a social security number), information relating to a person's race or ethnic origin, political opinions or religious beliefs, physical or mental health or condition, sexual orientation, trade union membership, genetic data and any related legal actions or the processing of biometric data for the purposes of uniquely identifying an individual. It may include information about an individual's criminal offences or convictions, as well as any other information deemed sensitive under applicable data protection laws. Where permitted by law and to the extent applicable, we may carry out background and/or criminal checks to determine your suitability for an open position or opportunity at VMware.

  We do not request sensitive personal information in connection with recruiting unless permitted or required by local law (for example for equal opportunity monitoring or internal policies related to diversity and anti-discrimination). Where required by applicable data protection or privacy law, we will obtain your consent to our use of your sensitive personal information.

Sources of information

- **Information we collect from you.** To process your application, we ask you to provide personal information about yourself. All information is provided on a voluntary basis, and you determine the extent of information you provide to us. However, some information may be necessary to complete an evaluation of your application and if it is not provided, our ability to consider you as a candidate may be limited.
- **Information we automatically collect.** We may automatically collect certain information from you about your visit to our Sites using "cookies" and other similar tracking technologies. For further information, please consult the VMware Cookie Notice.
- **Information from third parties.** We may obtain information about you from other sources to the extent permitted by applicable law, such as through your contact with us, including your interactions with us, or from third parties such as employment research firms, identity verification services, and other websites on the Internet (subject to such third party's privacy policies). For example, you may choose to provide us with access to certain personal information stored by third parties such as social media sites (for example, LinkedIn). In addition, and where this is relevant to your application, we may collect information from third parties who are lawfully entitled to share your information with us, for example, in connection with a background or employment check and/or an employment or work reference. By authorizing us to have access to this information, you agree that we may collect, store and use this information in accordance with this Applicant Notice.

PART II: How We Use Your Information

Personal information is used for the following purposes (unless restricted by applicable law):

- **Process Applications.** To process and evaluate your application, to assess and confirm your skills, qualifications and suitability for hiring, to make hiring decisions, to put together job offer and benefits packages, and to maintain accurate and up-to-date recruiting records.
- **Communicate.** To communicate with you about job opportunities, vacancies, applications and scholarship opportunities.
- **Manage Recruiting.** To run recruitment and promotion campaigns, and manage and improve our recruiting and hiring processes.
- **Background Checks.** To conduct reference and background checks where required and/or permitted by applicable local law.
- **Compliance.** To comply with corporate governance and legal and regulatory requirements, including equal opportunities monitoring. Some special categories of personal information, such as information about health or medical conditions, is processed to comply with employment law obligations (such as those in relation to candidates with disabilities and for health and safety purposes).

If you are hired, the information may be processed in connection with employment and corporate management (for example, to establish a basic employment record) in accordance with our Global Privacy Notice for Employees & Contingent Workers.

PART III: How We Disclose Your Information

We take care to allow your personal information to be accessed only by those who need access to be able to perform their duties, and to be shared only with third parties who have a legitimate purpose for accessing it. We may share your personal information with third parties as follows:

- **Service providers.** We may share your personal information internally and with service providers, vendors, agents and other third parties (for example, recruiters, consultants, analytics providers, attorneys and background checking services in connection with recruiting, employment, corporate governance, acquisitions and legal or regulatory requirements).
- **VMware affiliates.** We may share your information with our subsidiaries and other affiliates. This information will only be shared in connection with your recruitment and employment or contingent work as described in this Applicant Notice. We may also obtain information about you from our affiliated companies.
- **Vital interests.** We may disclose information where we believe it necessary in order to protect the vital interests of any person.
- **Compliance with laws or any competent law enforcement body, regulatory body, government agency, court or third party.** We may disclose information where we believe disclosure is necessary or required (i) by law or regulation, in order to comply with legal process or government requests (including in response to public authorities to meet equal opportunity laws, national security or law enforcement requirements); or (ii) to exercise, establish or defend our legal rights.
- **Business transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, acquisition, dissolution, corporate reorganization or similar event. We will inform any buyer that your information shall only be used in accordance with this Applicant Notice.
- **With your consent.** We may disclose your personal information for any purpose with your consent.

PART IV: Your Privacy Choices and Rights

We offer all individuals, regardless of residency, certain privacy choices. Residents of some territories (such as the European Economic Area or California) are afforded various additional privacy rights by applicable law.

Your choices

- **Communications from our Talent Acquisition Team.** You can opt-out of receiving communications from VMware's Talent Acquisition Team by adjusting your notification settings within your VMware Talent Community profile, available from careers.vmware.com. You can also opt out by clicking "unsubscribe" in any email communications we send you, or by submitting a request using our Privacy Contact Form (please reference this Applicant Notice in your request).
- **Correct or update your information.** If you would like to correct or update personal information that you provided to us, please logon to Talent Community at careers.vmware.com and update your profile.
- **Cookies and targeted advertising.** You may opt out of our use of cookies and similar technologies for various purposes such as targeted advertising. To do so, when you visit our websites, go to the cookie settings and turn off cookies per your preferences. Please see our Cookie Notice to learn more about cookies.

Your rights

Your rights may include:

- Access and portability. You may ask us to confirm whether we are processing your personal information, provide you with details about such processing, and, in some limited circumstances, give you a copy of your personal information. You may ask us to provide your personal information in a structured, commonly used, machine-readable format, or you can ask to have it ported directly to another data controller.
- Erasure or deletion. You may ask us to delete the personal information that we hold about you.
- Rectification or correction. You may ask us to correct any inaccurate or incomplete personal information that we hold about you.
- Objection to processing. You may request that we stop processing your personal information for specific purposes including marketing and profiling.
- Restriction of processing. You may request that we restrict the processing of your personal information in certain circumstances (for example, where you believe that the personal information we hold about you is not accurate or lawfully held).
- Appeal. You may have the right to appeal a decision we make regarding the exercise of your privacy rights.
- Lodge a complaint to your local Data Protection Authority. You may have the right to lodge a complaint with your national Data Protection Authority or equivalent regulatory body.
- Automated decision-making. We do not employ solely automated decision-making, as a matter of course, that results in automated decisions being taken (including profiling) that legally affect you or similarly significantly affect you. Automated decisions are decisions made automatically based on computer determinations (using software algorithms), without human review. If you are to be subjected to automated decision making, we will make it clear at the time and you have the right to contest the decision, to express your point of view, and to require a human review of the decision.

These rights are not absolute and are subject to conditions or limitations as specified in applicable laws. If you would like to exercise any of the above rights, please complete the Privacy Contact Form. We will process your request in accordance with applicable privacy and data protection laws. To protect your privacy and security, we may take steps to verify your identity before complying with the request.

PART V: Security and Confidentiality

We maintain (and require our service providers to maintain) appropriate organizational and technical measures designed to protect the security and confidentiality of any personal information we process. These measures include physical access controls, encryption, Internet firewalls, intrusion detection and network monitoring depending on the nature of the information and the scope of processing. VMware staff who may have access to personal information are required to keep that information confidential. However, no security procedures or protocols are ever guaranteed to be 100% secure so we encourage you to take care when disclosing personal information online and to use readily available tools, such as Internet firewalls, anti-virus and anti-spyware software, and similar technologies to protect yourself online.

Part VI: International Transfers

Personal information, including personal information collected from or about you may be transferred, stored and processed by us and our service providers, partners and affiliates in countries other than where your personal information was collected and other than where you reside, including the United States and other countries whose data protection laws may be different than the laws of your country. We will protect your personal information in accordance with this Privacy Notice wherever it is processed and will take appropriate steps to protect your personal information in accordance with this Privacy Notice and applicable laws. We have implemented similar appropriate safeguards with our service providers, partners and affiliates.

For transfers of personal information from our group companies in the EEA, the United Kingdom and Switzerland to our other group companies, we have implemented the Standard Contractual Clauses (issued by the European Commission or the UK's Information Commissioner's Office). Our Standard Contractual Clauses can be provided upon request.

PART VII: Deletion and Retention

We will retain personal information where we have a justifiable business need to do so and/or as long as is needed to fulfill the purposes outlined in this Applicant Notice, unless a longer retention period is required or permitted by law (such as tax, legal, accounting or other purposes). Specifically, our retention schedule categorizes records or information by department, content type, retention period, and any supplemental policies (domestic, regional and global) where applicable. Our retention schedule is based on a combination of laws and regulatory requirements, legal guidance, the amount, nature, and sensitivity of the personal information and to maximize operational efficiencies. We may also retain your information in accordance with applicable law to consider you for other job opportunities, unless you have told us that you do not wish us to retain your information for such purposes; we give you the opportunity to let us know if you do not want us to use your information for such purpose at the time that you provide your information to us. To the extent permitted or required by law, we may delete data at any time; accordingly, you should retain your own copy of any information you submit to us.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it, or, if this is not possible (for example, because your personal information has been stored in backup archives or for technical reasons), then we will securely store your personal information and implement appropriate measures to prevent any further processing until deletion is possible.

If you request deletion of your personal information (see "Your Privacy Choices and Rights" section for further information) we will consider your request in accordance with applicable laws.

PART VIII: Additional Notices and Disclosures for Certain Locations

California notice. Part XI sets forth our disclosure obligations under California law and provides further information about privacy rights for California residents.

Canada notice. VMware has appointed Stuart Lee, Chief Privacy Officer, to oversee compliance with this Privacy Notice and applicable privacy laws. For information on VMware's privacy practices, please contact Mr. Lee by completing the Privacy Contact

Form or by mail to: Stuart Lee, Chief Privacy Officer, VMware, Inc., 3401 Hillview Ave, Palo Alto, California, 94304, USA.

China notice. This additional China Privacy Notice sets forth our disclosure obligations under Personal Information Protection Law of the People's Republic of China ("PIPL").

European Economic Area and UK – legal basis for processing personal information. Our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it. We will normally collect personal information from you to comply with our contractual obligations to you or to take steps to enter into a contract with you, if the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms, or if we have your consent to do so. In rare cases, we may have a legal obligation to collect personal information from you or may otherwise need the personal information to protect your vital interests or those of another person. We may sometimes provide you with additional information about this legal basis at the time this information is collected. See Part II, 'How We Use Your Information', for more details regarding the purposes for which we process your personal information. To process your personal information for such purposes, we typically rely on our legitimate interests in recruiting and assessing applicants; in providing information and resources to prospective employees, workers, interns and scholarship recipients; in promoting VMware to applicants; and in improving the functionality, effectiveness, and security of our recruitment resources and processes. As applicable, we may also rely on your consent, or such processing may be necessary for the performance of a contract.

PART IX: Other Information

External links and social media features. Our online Sites may provide links to or the ability to connect with third-party websites, services, social networks, applications or social media features such as "Share" or "Like" buttons. Visiting those sites or clicking on those links may allow the third party to collect and use information about you. Further, the personal information you choose to give to these third parties is not covered by this Applicant Notice. We encourage you to review the privacy notices and terms of use of such third parties prior to interacting with them or providing them with your personal information to understand how your information may be collected and used. We do not control the privacy practices of such third parties, nor do we endorse or make any representations about these third-party websites, services, social networks or applications.

Changes to this Applicant Notice. We will review and update this Applicant Notice periodically in response to changing legal, technical and business developments. When we update this Applicant Notice we will note the date of its most recent revision above. If we make material changes to this Applicant Notice, we may take appropriate measures to inform you in a manner that is consistent with the significance of the changes we make and is in accordance with applicable law. We encourage you to review this Applicant Notice frequently to be informed of how we are protecting your information.

Your responsibilities. You are responsible for the information you provide or make available to us, and you must ensure it is honest, truthful, accurate and not misleading in any way. You must ensure that the information provided does not contain material that is obscene, defamatory, or infringing on any rights of any third party; does not contain malicious code; and is not otherwise legally actionable. Further, if you provide any information concerning any other person, such as individuals you provide as references ("referee"), you are responsible for providing any notices and obtaining any consents

necessary for us to collect and use that information as described in this Applicant Notice before you provide the referee's personal information to us.

PART X: How to Contact Us

If you have any questions or concerns regarding this Privacy Notice, you may submit a request using our Privacy Contact Form or write to us by mail to: Office of the General Counsel, 3401 Hillview Ave, Palo Alto, California, 94304, USA. Please reference this Applicant Notice in your communication.

Part XI: California Privacy Rights

This Part sets forth additional disclosures pursuant to California law, including the California Consumer Privacy Act of 2018 as amended ("CCPA") and the California Civil Code section 1798.83. This section provides additional details regarding the information defined under applicable California law as 'personal information' of applicants who are California residents. Except where we have made a distinction, references to 'personal information' include 'sensitive personal information', as defined by applicable California law.

1. Categories of personal information collected and purposes for collection and use

We have collected the following categories of personal information in the preceding 12 months, for the following purposes.

For further information about these purposes see above at PART II: How We Use Your Information.

Category of Personal Information (*corresponds to categories listed in CCPA §1798.140(v)(1)*)	Examples	Purpose of Collection and/or Use
Identifiers	Name, address, email address and government-issued identifier (e.g., social security, passport, visa numbers)	Process Applications Communicate Manage Recruiting Background Checks Compliance
Personal information listed in § 1798.80 of the California Customer Records statute (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, education, employment, employment history, bank	Name, social security number, address, telephone number, passport number, education, employment, employment history	Process Applications Communicate Manage Recruiting Background Checks Compliance

account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information)		
Characteristics of protected classifications under California or federal law	Race, national origin, age, mental and physical disabilities, sex, pregnancy or related conditions, medical condition, marital status, military or veteran status. This information may be collected for purposes such as accommodations; our diversity, equity and inclusion initiatives; or monitoring compliance with laws or satisfying reporting obligations. Often the information is voluntarily shared by you, and not required or requested by us.	Process Applications Manage Recruiting Background Checks Compliance
Commercial Information	Products or services purchased or obtained, transaction information and purchase history. This information may be collected if submitted for reimbursement or otherwise related to your application.	Manage Recruiting
Internet or other electronic network activity information	Browsing history and information regarding interaction with our online Sites	Manage Recruiting
Geolocation data	Approximate physical location (derived from an Internet Protocol address)	Manage Recruiting
Audio, electronic, visual, thermal and similar information	Photographs and any other audio/visual information that candidates voluntarily submit to us as part of an application, or that are included in social media profiles (e.g., LinkedIn)	Process Applications
Professional or employment-related information	Work history, prior employers, professional certifications, courses and memberships.	Process Applications Manage Recruiting Background Checks

		Compliance
Education information	Academic records, disciplinary records and other records related to a student	Process Applications Manage Recruiting Background Checks Compliance
Inferences drawn from the any of the above	Professional aptitude and professional abilities	Process Applications Manage Recruiting Compliance
Category of Sensitive Personal Information (*corresponds to categories listed in CCPA §1798.140(ae)*	**Examples**	**Purposes of Collection and/or Use**
Identification numbers	Social security number, driver's license or passport number	Process Applications Manage Recruiting Background Checks Compliance
Account credentials	Account log-in and passwords or credentials allowing access to application-related accounts. Passwords are hashed and encrypted into a form that allows for authentication, but not account access.	Manage Recruiting
Personal information that reveals a consumer's racial or ethnic origin or religious beliefs	This information may be collected for purposes such as accommodations, our diversity, equity and inclusion initiatives; and monitoring compliance with laws or satisfying reporting obligations. Often the information is voluntarily shared by you, and not required or requested by us.	Process Applications Manage Recruiting Compliance
Email and text messages unless we are the intended recipient	We do not intentionally collect any emails or texts where we are not the intended recipient, *i.e.*, emails and texts that are not business-related.	n/a

2. Personal information sources

With respect to each category above, your personal information is generally collected from you and/or from third parties except that internet or other electronic network activity

information and IP address are collected automatically. See PART I: What information we collect & how we use it; Sources of information.

3. Retention of personal information

With respect to all categories of personal information, see Part VII: Deletion and Retention. If we de-identify or anonymize your personal information, we will maintain and use it in de-identified form and not attempt to re-associate the information with you, except to test our de-identification procedures.

4. Disclosure of personal information

With respect to all categories of information, we may disclose, and have disclosed in the preceding 12 months, personal information to our affiliates and to vendors, consultants, service providers and agents for operational business purposes such as to enable vendors to perform services on our behalf, to coordinate efforts among VMware entities, or to facilitate recruiting efforts. For further information see PART III: How We Disclose Your Information.

5. Personal information sold or shared

We do not sell or share personal information for monetary consideration. However, under California law, some uses of cookies and similar tracking technologies may be characterized as "selling" or "sharing" personal information. Because we use such technologies with our websites and applications, in the preceding 12 months we may have "sold" or "shared" the following categories of personal information for recruiting or marketing purposes such as to serve advertisements, to analyze the success of recruiting campaigns, or to understand the use of our websites, and such receiving entities may use the personal information for their own purposes, such as to improve their ability to target advertisements. The following personal information is "sold" or "shared" to advertising networks, social media networks and analytics partners.

Category of Personal Information Sold or Shared (*corresponds to categories listed in CCPA §1798.140(v)(1)*)	Examples
Identifiers	Online/cookie identifier, Internet Protocol address, or other similar identifiers Internet Protocol address may be used by the receiving entity to derive your approximate physical location
Internet or other electronic network activity information	Website activity, web pages viewed, source and medium (paid/organic) to website, path through website, emails opened, downloads of files offered online, browser, operating system characteristics

We do not have actual knowledge that we sell or share the personal information of applicants under 16 years of age.

6. Your rights under the CCPA

Under the CCPA, you may have the following rights. Please note that these rights are not absolute and are subject to conditions or limitations:

Right to Know (Collection). You have the right to request that we disclose to you the categories and specific pieces of personal information we have collected about you.

Right to Know (Collection and Disclosure). You have the right to request that we disclose certain information about how we have handled your personal information, including the:

- categories of personal information collected about you (see above);
- categories of sources from which we collected your personal information (see above);
- business and/or commercial purposes for collecting, selling, sharing and/or disclosing your personal information (see above);
- categories of third parties to/with whom your personal information has been disclosed, including for a business purpose (see above);
- categories of third parties to/with whom your personal information has been sold or shared (see above); and
- the specific pieces of personal information collected about you.

Access and Portability. You have the right to obtain a list of categories and a copy of the personal information collected about you, in a portable and (if technically feasible) readily usable format.

Deletion. You have the right to request the deletion of your personal information we have collected from you. This right may be subject to certain conditions and limitations under the law.

Correction. You have the right to request the correction of your personal information that we maintain.

Right to Opt-Out of Selling or Sharing. We do not sell or share personal information for monetary consideration. However, under California law, some uses of cookies and similar tracking technologies may be characterized as "selling" or "sharing" personal information. You have the right to opt-out of such "selling" or "sharing" of your personal information. To exercise this right, when you visit our online Sites, go to the cookie settings (accessible via a "Do Not Sell or Share My Personal Info" button or link) and turn off cookies per your preferences. Because your cookie preferences are tied to your device and browser, if you visit our website from a different device or browser, or clear cookies or settings on your browser, you will need to re-select your preferences.

Right to Limit the Use of Sensitive Personal Information. Such right is not applicable as we do not collect or process sensitive personal information for the purpose of inferring characteristics about you. We do not, as a matter of course, use or disclose sensitive personal information for purposes other than those specified in Section 7027(m) of the

California Consumer Privacy Act Regulations. Such permitted purposes include the performance of services reasonably expected by an average applicant who requests those services; to prevent, detect and investigate security incidents; to resist malicious, deceptive, fraudulent or illegal actions directed at us; to ensure the physical safety of natural persons; short-term, transient uses such as nonpersonalized context-based advertising; to verify, maintain or improve the quality of a service; and purposes that do not infer characteristics about the applicant.

Right to be Free from Discrimination. We will not unlawfully discriminate against you for exercising your rights under the CCPA.

7. Exercising Your Rights

To exercise your rights as set out above, please contact us by:

- calling 1-877-486-9273, option 0, or
- by submitting a request here.

Depending on the sensitivity of your request, you may be required to provide additional information to verify your identity and request before further action is taken. If your request is for access to your personal data, we will confirm your email and one or more additional pieces of information provided in your request to verify against information already in our possession, such as name and state or country of residence. If we are unable to confirm that the data provided in your request matches our records, we will ask for additional information to verify your identity.

Your authorized agent may make a request on your behalf. We will consider any evidence the agent submits to demonstrate that you gave the agent signed permission to submit the request. We may email you to confirm that the agent is indeed acting on your behalf.