SHARTSIS FRIESE LLP

**PRIVACY NOTICE**
**FOR PERSONNEL AND BUSINESS CONTACTS**

**YOUR RIGHTS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)**

*Effective January 1, 2023*

This privacy notice ("Notice") describes how Shartsis Friese LLP (collectively, "Shartsis," "we," "us," and "our") collect, use, and share personal information about California residents who engage with Shartsis either in a human resources or business-to-business capacity, including employees (which for purposes of this notice only includes partners), former employees, and other personnel and any of their emergency contacts, health plan members, and beneficiaries; non-employee staff, independent contractors, advisors, directors, owners, shareholders, job applicants, contacts at current and prospective business customers, vendors and partners, event attendees and office visitors, and other individuals whose personal information is stored or processed in human resources information systems, customer relationship management (CRM) systems, and contact management systems.

## 1) Scope

This Notice applies only to "personal information", as defined in the California Consumer Privacy Act of 2018 as amended including by CPRA (the "CCPA"), that we collect to the extent we qualify as a "business" as defined in the CCPA but does not apply to personal information excluded from the scope of the CCPA.

This Notice does not apply to you if you are not a California resident or you are otherwise not entitled to a notice under CCPA. In addition, this Notice does not apply to personal information covered by a different privacy notice that we give to California residents, such as the privacy notices we give to our website visitors or product or services users.

Information you provide directly to another party is not covered by this policy. Examples of this would be if we pay for your subscription to a meditation app as a wellness benefit and you set up and use an account with that app. Or if we pay toward the premium for a health, life, or disability insurance. Your activity with that policy that you establish is between you and the insurer except as relevant for our financial contribution.

## 2) Personal Information We Collect

### a) Employees

i) *Administration of our Relationship.* The sort of information we hold includes your application form and references, your contract of employment and any amendments to it; correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary; information needed for payroll, benefits (such as disability, health, and life insurance) and expenses purposes; contact and emergency contact details; records of holiday, sickness, and other absence; information needed for equal opportunities monitoring policy; and records relating to your career history, such as training records, appraisals, other performance measures, and, where appropriate, disciplinary and grievance records.

To administer our operations we collect the following data from employees: real name, alias, usernames, postal address, unique personal identifier, Internet Protocol address, email address, telephone number, account name, Social Security Number, driver's license number, passport number, bank account number, insurance policy number, credit card number, debit card number. And the following data collected from your engagement as an employee: Job related data, maintained as part of the employment relationship that could be contained in a job application or resume; an employment contract; a contractor agreement; a performance review; a disciplinary record; compensation information; information relating to vacation, sick time, personal time and other absences and leaves of absence; photos; information from employee expenses; payroll and benefits-related data; internal and external contact information; or information captured from video, audio, or other forms of monitoring or surveillance.

As part of our verification of background process, we may collect your education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades or transcripts.

We use this information to conduct our operations as a business.

ii) *Information Generated in the Course of Your Employment.* You will, of course, inevitably be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company such as emails, messages (like Slack), intranet platforms and customer relationship management platforms (like Salesforce), client or customer communications, blog posts, marketing materials. Your image and name will be broadcast on videoconferences (such as zoom or Google meets). We use this information to conduct our operations as a business.

iii) *Health Information.* Where necessary, we may keep information relating to your health, which could include reasons for absence and physician reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations – to consider how your health affects your ability to

do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and company sick pay and to facilitate emergency procedures such as in the event of an evacuation. *Potentially Sensitive Information.* Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data, or sexual orientation, we will always obtain your explicit consent to those activities unless this is not required by law, or the information is required to protect your health in an emergency. We collect: Information relating to age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, and requests for parental, pregnancy, disability or sick leave. Your voice may be recorded as part of your voicemail greeting and messages you send other employees.

Where we are processing data based on your consent, you have the right to withdraw that consent at any time. While the circumstances will vary, we would likely process this information for purposes such as diversity initiatives and where legally required. We may receive this information in an inferred format. For example, the gender of your spouse on health insurance forms would allow us to infer your sexual orientation. We do not use inferred sensitive information.

iv) *Automated Monitoring.* In addition, we may monitor computer usage such as browsing history, search history, information on an employee's interaction with a website or application, or an employee's public postings on the Internet, including social media sites.

**b) Personnel and Non-Personnel**

i) *Contact Information.* As a business, we receive personal information such as your name, email, and title if you provide us this information when you attend an event, visit one of our sites, are a prospective customer, work for us as a consultant, or are a contact at a vendor. [Disclose any purchase of leads or lists.] We use this information to communicate with you and conduct our business relationship.

ii) *Benefits Administration.* We may offer benefits to the family members of employees (such as health insurance or subscriptions to wellness or meditation apps) and we may offer employees benefits that allow them to designate beneficiaries to those benefits (such as life insurance policies or 401k plans). We use this information to administer these benefits.

iii) *Operations.* Our employees may list emergency contacts and references. We use this information to operate our business.

iv) *Security.* We have various physical, technical, and administrative security measures to protect our premises, employees, and technology. These include video cameras in the exterior and interior of our buildings; badges to enter the building, elevators, loading docks, and office spaces; sign-in processes for guests to our facilities. We use this information for security purposes.

## 3) Sources of Personal Information

### a) Employees

Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager, or in some cases, external sources (such as credit agencies, background check providers, recruiters, and referees) or automated sources (such as monitoring information that your work computer or mobile device transmits when interacting with our software or technology).

### b) Non-Employees

Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your business contact at the Firm or an employee with whom you have a relationship.

## 4) How We Use Personal Information

We use your personal information under this Notice to operate our business. For example, we may use your personal information for fraud prevention, administrative and legal purposes, marketing and business communications to customers and potential customers, manage our relationship with our contractors, consultants, and business partners/vendors, or reporting potential crimes.

We may also use personal information for other purposes consistent with the Notice (for example, we noted our uses in several sections above where we described types of data collected) or that are explained to you at the time of collection of your personal information.

If we are your employer or you work for us in another capacity, such as a consultant, the Company needs to keep and process information about you for normal employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends, and after you have left. This includes using information to enable us to comply with the employment contract, comply with any legal requirements, pursue the legitimate interests of the Company, and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some

circumstances to comply with our obligations, and we will tell you about the implications of that decision.

In the interest of providing additional detail, the Firm may use or disclose personal information that we collect about you for one or more of the following business purposes:

- as part of our recruiting and onboarding of new employees;
- to conduct employment related background screening and checks;
- to administer benefits, such as medical, dental, optical, commuter, and retirement benefits, including recording and processing eligibility of dependents, absence and leave monitoring, and insurance;
- to pay or to reimburse for expenses, including salary administration, payroll management, payment of expenses, to administer other compensation related payments, including assigning amounts of bonus payments to individuals;
- to monitor work-related licenses and credentials, including provisioning software licenses for use in the course of an employee's work-related responsibilities, ensuring compliance, training, examination and other requirements are met with applicable regulatory bodies;
- to provide human resources management services, including providing employee data maintenance and support services, administration of separation of employment, approvals and authorization procedures, administration and handling of employee claims, and travel administration;
- to maintain your contact information;
- to assist you in the case of an emergency, including maintenance of contact details for you, and your dependents or emergency contacts in the case of a personal or business emergency;
- to foster and improve our culture and working environment, including conducting staff surveys, providing senior management information about other employees, and conducting training;
- to ensure a safe working environment, which includes information collected relating to disciplinary actions, and code of ethics conduct processes and investigations;
- to protect health and safety in the workplace, including conducting surveys and health screenings involving collection of personal health information about you and your

household, to permit contact tracing and reduce the risk of spreading viruses or other diseases during a pandemic or public health emergency;

- to maintain security on the Firm systems and infrastructure, which includes hosting; management of our software and hardware computer assets; systems testing, such as development of new systems and end-user testing of computer systems; training; and monitoring email and internet access; and

- to comply with applicable law or regulatory requirements, such as legal (state and federal) and internal company reporting obligations, including headcount, management information, demographic and other required reporting.

**5) How We Disclose Personal Information**

We may disclose for business purposes all of the categories of personal information described above with the following categories of third parties:

**a) Service providers.** Companies that provide us with services that help us provide services or operate our business, such as payroll providers, health insurance providers, employee wellness and health benefits providers, financial services providers (for example, institutions that manage our 401k program or offer life insurance and disability insurance benefits), travel concierge providers, IT and software services (email, videoconferencing, document management, messaging, telecommunications providers (phone, messaging, internet access), cloud hosting/storage services, website hosting, mailing services, marketing services, event management services, professional development and management coaching providers, cyber security services, office security services.

**b) Government entities and law enforcement.** Government authorities, law enforcement, courts, and others for legal purposes such as those identified above. For example, if an employee is getting divorced, we may receive a subpoena for employment records that describe dates of employment, annual compensation, and position. When we disclose your personal information to comply with a legal obligation or legal process, we will take reasonable steps to ensure that we only disclose the minimum personal information necessary for the specific purpose and circumstances.

**c) Corporate transaction participants.** Parties to transactions and potential transactions for the sale, transfer or licensing of a portion or all of our business or assets, including your personal information, such as a corporate divestiture, merger, consolidation, acquisition, reorganization or sale of assets, or in the event of bankruptcy or dissolution.

**d) Professional advisors.** Our lawyers, accountants, bankers, and other outside professional advisors in the course of the services they provide to us.

e) **Other.** We may also share personal information with other categories of third parties with your consent or as described to you at the time of collection of your personal information.

## 6) Selling or Sharing Personal Information

We do not believe that we “sell” or "share" your personal information as defined in the CCPA. We engage a number of vendors to operate an efficient and successful enterprise. It is a priority in the near term to review our contracts with our vendors and to limit their ability to process personal information for any purpose other than to provide us the contracted services or to improve the products and services we are receiving.

## 7) Security Practices

The security of your personal information is important to us. We employ a number of organizational, technical and physical safeguards designed to protect the personal information we collect. However, security risk is inherent in all internet and information technologies, and we cannot guarantee the security of your personal information.

## 8) Do Not Track.

Some Internet browsers may be configured to send “Do Not Track” signals to the online services that you visit. We currently do not respond to “Do Not Track” or similar signals. To find out more about “Do Not Track,” please visit www.allaboutdnt.com. This is distinct from our response to opt-out signals such as Global Privacy Control (aka GPC) under the California Consumer Privacy Act and other state privacy laws, if applicable.

## 9) Minors

The Firm does not employ or contract with children, and we do not knowingly collect personal information from children under the age of 16 except where they are listed as beneficiaries of a health insurance plan, may visit our site to visit parents or attend an event, or other administrative purpose related to our relationship with an adult employee or other personnel. We do not knowingly share the personal information from children under the age of 16 for cross-context behavioral advertising nor do we sell that information. If we find out that a child under 16 has given us personal information except for the administrative purposes listed above, we will take steps to delete that information. If you believe that a child under the age of 16 has given us personal information, please Contact us at ccpa-rights@sflaw.com You may also call us collect at (415) 421-6500 and ask for Jim Schwarz, Chief Operating Officer. Leave a message with the receptionist or on his voicemail if Jim does not answer.

**10) Sensitive Personal Information**

The Firm does collect sensitive personal information from employees and other personnel including Social Security Number, passport number, biometric information used to uniquely identify the individual, information about sex life or sexual orientation (which can be inferred from benefits and emergency contacts), the contents of an individual's mail, email, and text messages (unless the business is the intended recipient), other government-issued identification details (like from a California driver's license), and health conditions that may impact mobility in the event of an evacuation.

We do not use or disclose sensitive personal information other than as needed to provide normal and customary employer functions, like payroll, verification of employment-eligibility, health insurance benefits, tax functions, and emergency preparedness and evacuations protocols and as permitted by California law. To its knowledge, the Firm does not sell or share sensitive personal information for the purpose of cross-context behavioral advertising.

**11) De-identified Information**

Personal information does not include information that is deidentified. When we receive or use deidentified information, we maintain it in deidentified form and do not attempt to reidentify the information.

**12) No Financial Incentives**

We do not offer financial incentives to you based upon the retention or sale of your personal information.

**13) Retention of Personal Information.**

We retain your information to operate our business. Our vendors determine the retention policy for much of the data we collect, particularly for non-employees. It is a priority of the Firm to determine and shorten retention periods for personal information.

Employees. We retain transactional information such as proof of your identity and ability to work in the United States and your banking and tax details for at least seven years to ensure we can perform legitimate business functions, such as accounting for tax obligations. We also retain your information as necessary to comply with our legal obligations, resolve disputes, and enforce our terms and policies.

**14) Exercising Your Rights**

California law provides some California residents with the rights listed below. To exercise these rights, see the “Exercising Your California Privacy Rights” section below. You also have the right to exercise these rights free of discrimination.

These rights are subject to various exceptions and limitations as provided in the law. If you wish to exercise your rights, please contact us at privacy-requests@sflaw.com.

a) **Right to Know**. You have the right to know and see what personal information we have collected about you, including:

   - The categories of personal information we have collected about you;
   - The categories of sources from which the personal information is collected;
   - The business or commercial purpose for collecting or sharing your personal information;
   - The categories of third parties with whom we have disclosed your personal information; and
   - The specific pieces of personal information we have collected about you.

b) **Right to Delete.** You have the right to request that we delete the personal information we have collected from you (and direct our service providers to do the same).

c) **Right to Correct.** You have the right to request that we correct inaccurate personal information.

d) **Right to Opt Out.** You have the right to opt out of certain uses and sharing of personal information, including any sale of personal information, sharing of personal information for cross-contextual behavioral advertising purposes, or use of sensitive personal information for certain purposes (e.g., use or disclosure beyond what is reasonably necessary to provide the services or provide the goods reasonably expected by an average consumer).

e) **Other Rights.** You can request certain information about our disclosure of personal information to third parties for their own direct marketing purposes during the preceding calendar year. This request is free and may be made once a year. You also have the right not to be discriminated against for exercising any of the rights listed above.

f) **Exercising Your California Privacy Rights.** To request access to or deletion of your personal information, or to exercise any other privacy rights under California law, please contact us at ccpa-rights@sflaw.com or call us collect at (415) 421-6500 and ask for Jim Schwarz. Leave a message with the receptionist or on his voicemail if Jim does not answer.

g) **Verification of Your Identity.** To respond to some rights, we may need to verify your request. If you do not have an employee email account with us, additional information to verify your identity may be required by law before we may act upon a request. This additional information may vary depending on the nature of your request and the nature of the information you are requesting. In some cases, we may also be required by law to obtain a signed declaration under penalty of perjury from you attesting that you are the subject of the request. If we suspect fraudulent or malicious activity on or from your account, we will delay acting on your request until we can appropriately verify your identity and the request as authentic.

You may designate an authorized agent to make a request on your behalf pursuant to applicable law. We accept documentation of your designation in the form of a valid power of attorney or a notarized statement. We may require verification of your authorized agent in addition to the information for verification above for consumers and households.

h) **Response Timing and Format.** We aim to respond to a consumer request in relation to these rights within 45 days of receiving that request. If we require more time, we will inform you of the reason and extension period in writing.

i) **Use of Verification Information.** Information that you submit for the purpose of allowing us to verify your identity in furtherance of a consumer-related or household-related request pursuant to California law will only be used by us, and our service providers if any, for that purpose and no other. Except where we are required by or advisable under law to maintain this information for record-keeping purposes, we will take steps to delete any new personal information collected for the purpose of verification as soon as practical after processing your request.

j) **Exceptions.** Please also be aware that making a request does not ensure complete or comprehensive removal or deletion of Personal Information or content you may have posted, and in some circumstances the law does not require or allow us to fulfill your request. This may occur where fulfilling your request may infringe upon the rights and freedoms of other consumers.

**15) Request Fees.**

We reserve the right to charge a reasonable fee or take other appropriate action in response to requests from a consumer or household that are manifestly unfounded or excessive, in particular because of their repetitive character.

**16) Changes to Practices**

If in the future we intend to process your personal data for a purpose other than that which it was collected we will provide you with information on that purpose and any other relevant information. We may amend this Privacy Policy by posting the amended version in this location and indicating the effective date of the amended version. We may announce any material changes to this Privacy Policy through our normal means of communicating with you.

**17) Contact**

If you have any concerns as to how your data is processed you can contact us at ccpa-rights@sflaw.com or call us collect at (415) 421-6500 and ask for Jim Schwarz, Chief Operating Officer. Leave a message with the receptionist or on his voicemail if Jim does not answer.