Privacy Statement

This Privacy Statement (the “Statement”) describes how we collect and process your Personal Data. This Statement is issued for all companies doing business as GenSphire LLC. When we refer to "GenSphire," or "we", "our," or "us" in this Statement, we are referring to GenSphire®, responsible for processing your Personal Data. This Statement supplements any other privacy notices and policies and is not intended to override them, including, but is not limited to, any provisions in the Employee, Consultant, and Vendor Handbook.

For purposes of this Statement,

> “Full Time” means an individual who works, or is applying to work, for a client of GenSphire, and that client is a company to which GenSphire provides services.
>
> “GenSphire Employee” means an individual who works, or is applying to work, for GenSphire in the capacity of an employee internally at GenSphire.
>
> “GenSphire Vendor” means a company, independent professional, or organization that works, or is requesting to work, for GenSphire in the capacity of a vendor.
>
> “Contractor” means an individual who works, or is applying to work, for GenSphire in the capacity of a GenSphire Vendor whom GenSphire assigns to work at GenSphire’s clients.
>
> “Consultant” means a GenSphire Vendor.
>
> “Personal Data” means any information that identifies relates to, describes, or is reasonably capable of being linked directly to any individual or household.
>
> “Processing” means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

This Statement Describes:

Personal Data we collect

The categories of Personal Data collected may include the following:

Identifiers, such as your name, username or similar online identifier, password, employee/staff ID, date of birth, Social Security number or equivalent national identification number, driver's license, California or other state identification card, passport number, or other government-issued identification card.

Contact Information, such as your work and home addresses, telephone numbers, email addresses, and emergency contact details.

Characteristics of protected classifications under California, provincial or federal law, such as your race, age, gender, national origin, citizenship, self-identification of disability, request for leave for family care, health condition, pregnancy, military or veteran status, and marital status.

Information about your job, such as job title, category and status, work location, department, employment contract, assigned tasks and projects, weekly hours, supervisor's name, start and end date, and reason for leaving.

Education information, such as your education and training background.

Professional or employment related information and documents, such as prior work experience and any other information that may be included in your resume or job application, training, confidentiality agreements, and proprietary rights agreements.

Internet and other electronic network activity information, such as information about how you use our website, products and services using cookies (as discussed further below),

IT systems usage information related to your use of our equipment, systems, and other resources.

Audio and visual information, such as photographs and phone and video recordings.
Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences, email content, business letter content, business documents, and chat content.
Data Voluntarily Submitted including any data that you voluntarily submit through contact forms, resume, or cover letter.

Performance and disciplinary information, such as performance reviews, evaluations and ratings, information about disciplinary allegations, the disciplinary process and any disciplinary warnings, details of grievances, and any outcome.

Information about your compensation and benefits, such as your basic salary, bonus and commission entitlements, insurance benefits (including information about you and your dependents that we provide to the insurer), hours and overtime, tax code, holiday entitlement, accrued salary information, and information relating to your pension.

Family Information, such as the marital status, name, relationship, date of birth, and social security numbers of your family members and any other information that may be needed for the administration of benefits, and contact details to identify who to contact in the case of an emergency.

Financial information, such as your bank details (for payroll, payments and travel reimbursement purposes only) and business travel and entertainment data.

Health information, as required by law or as necessary to manage the employment relationship, including benefits administration, occupational health, disability accommodation, Consultants' compensation, and leaves of absence.

Union membership status, as required by law to ensure benefits, terms of employment, and employment policies comply with the Union's requirements or any relevant collective agreement.

Termination and Post-Employment Information, such as termination agreements, benefits notices, and unemployment compensation forms.

Sensitive Personal Information

We collect Personal Data that is defined as "Sensitive Personal Information" under applicable privacy laws, including driver's license, state identification card, passport, or other government issued identification card, social security numbers, race or ethnic origin, citizenship, immigration

status, and health information. We use and disclose Sensitive Personal Information only as necessary: (i) to process your request for employment, (ii) provide services and benefits in connection with your employment, (iii) to comply with the law, and (iv) for business purposes reasonably expected within the scope of your employment.

Retention

For each of these categories of Personal Data, we will retain the information as long as is reasonably necessary to fulfill the purpose for which it was collected and to comply with applicable laws and regulations. We consider the following criteria when determining how long to retain Personal Data: why we collected the Personal Data, the nature of the Personal Data, the sensitivity of the Personal Data, our legal obligations related to the Personal Data, and the risks associated with retaining the Personal Data.

Client Data Collection

This Statement is directed solely to our collection and use of your Personal Data. Clients of GenSphire may also collect the Personal Data of Full Times and Temporary Employees, and any such collection and use by clients shall be governed by the client privacy policies.

If You Do Not Provide Personal Information. Where we need to collect Personal Data by law, in order to perform our services, or pursuant to a contract we have with you, and you do not provide that data when requested, we may not be able to perform the services or contract we have or are trying to enter into with you (for example, to provide you with products or services). In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

Information You Provide To A Third Party

Our website includes links from the website to, and plug-ins (such as Facebook, BlueSky, and LinkedIn buttons) from, sites or applications operated by third parties (“Third-Party Sites”). GenSphire does not control any Third-Party Sites and is not responsible for any information they may collect. Its privacy Statement governs the information collection practices of a Third-Party Site. It is your choice to enter any Third-Party Site. We recommend that you read its privacy Statement if you choose.

Children’s Privacy

Our website and online services are intended for adult use only and are not directed towards children, minors, or anyone under the age of 18. If you are under the age of 13, you are not authorized to provide us with any Personal Data. If the parent or guardian of a child under 13 believes that the child has provided us with any Personal Data, please contact us at the email address below and ask to have this Personal Data deleted from our files.

HOW WE COLLECT YOUR PERSONAL DATA

We may collect your Personal Data from a variety of sources and methods. This includes:
Information You Voluntarily Provide to Us
We collect Personal Data from you that you voluntarily provide to us, including when you:

- Fill out a Contact Us form;
- Subscribe to our publications;
- Create an account;
- Request marketing materials;
- Request reminders to apply for an open position;
- Fill out an employment application and during the scope of your employment;
- Give us feedback; or
- Attend any of our events, promotions, or other programs where we collect information about you.

Information We Collect When You Use Our Systems:

We collect Personal Data when you use our systems, including computer systems, security systems, time keeping systems, and any internal intranet or online platforms.
Information We Collect When You Use Our Website

Automated technologies or interactions. If you use one of our websites, we receive and store internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and/or clickstream data. When you access and use our website from your mobile devices, we receive data from that mobile device. This may include your device ID, location data, IP address and device type. You may manage how your mobile device and mobile browser share location information with us, as well as how your mobile browser handles cookies and related technologies by adjusting your mobile device privacy and security settings. Please refer to instructions provided by your mobile service provider or the manufacturer of your device to learn how to adjust your settings.
Cookies. Our websites may also place cookies on the device that you use to access the websites. Cookies are small files that we or our service providers transfer to your device through your web browser that enables us or our service providers' systems to recognize your browser and capture and remember certain information. We use cookies to help us understand how users use the website. For example, cookies gather information about how long you spend on a web page so that we can understand what web pages are of most interest to users. If you prefer, you can opt out of cookies when you visit our website through the cookies pop up that appears when you visit our website by choosing to decline cookies and also choose to have your computer warn you each time a cookie is being sent, or you can choose to turn off cookies by adjusting your browser settings. If you turn off your cookies, some of the features of the website may not function properly.

Google Analytics.

We use Google Analytics to assist us in better understanding our website visitors. Google Analytics uses a first party cookie, identifiers for mobile devices, or similar technology to collect usage data. Based on this information, Google Analytics compiles data about website traffic and interactions, which we use to offer better user experiences, perform analytics, analyze traffic, personalize content, and offer ads that match your interest. You can learn more about how Google Analytics collects and uses information from their website at: www.google.com/policies/privacy/partners/.

HOW WE USE YOUR PERSONAL DATA

GenSphire uses Personal Data for all purposes related to the creation, administration, and termination of GenSphire Employees' and contractors' employment relationship with GenSphire and for all purposes related to vetting Full Times to work at GenSphire's clients. These purposes include, but are not limited to, the following:

To respond to requests for information.
To evaluate feedback and complaints.
To communicate with users, e.g., to communicate with applicants applying for jobs.
To evaluate applicants for internal jobs.
To evaluate applicants for consulting assignments with GenSphire's clients.
To improve our products and services.
To continuously evaluate and improve the online experience.
To prepare headcount reports and other reports related to GenSphire;
To administer employee compensation, including, but not limited to, payment of wages and bonuses and income tax withholding and reimbursement of business expenses;
To administer employee benefits;
To administer performance appraisals, safety, and travel arrangements;
To manage and administer pay adjustments or periodic bonuses;
To administer leaves of absence as required by law or company Statement;
To monitor and enforce compliance with internal policies;
To provide employee contact information to current and prospective customers;
To engage in succession planning;
To administer training of employees of the GenSphire;
To comply with mandatory government reporting requirements;
To provide Help Desk support to employees of GenSphire worldwide; and
If you are a Temporary Employee: to place you with clients by matching your qualifications against the client's staffing needs; to manage and administer the assignment to a client; and to create reports, including reports detailing turnover and retention rates.
For recruitment purposes;
To assess qualifications of applicants and eligibility to work in the US or Canada, as applicable;
To administer secure access to our IT resources worldwide;
For emergency contact purposes;

To conduct audits as required by law;
To resolve issues submitted to GenSphire;
To exercise GenSphire's rights under applicable law and to support any claim, defense, or declaration in a case or before a jurisdictional and/or administrative authority, arbitration, or mediation panel;
To meet legal and regulatory requirements including civil discovery in litigation involving GenSphire;
To facilitate administrative functions, including, but not limited to, the management and operation of information technology and communications systems, risk management and insurance functions, budgeting, financial management and reporting, strategic planning, and the maintenance of licenses, permits and authorizations applicable to GenSphire's customers'/clients' business operations; and equal opportunities monitoring.

HOW WE DISCLOSE PERSONAL DATA

Information You Direct Us to Disclose

You may be presented with an option on our service to have us send certain information to third parties or give them access to it. If you choose to do so, your Personal Information and other information may be disclosed to such third parties. Additional, when you apply for a position, we disclose Personal Data for contractors and Full Times to clients for the purposes of evaluation, hiring, placement, and to comply with legal obligations but only to the extent required to meet these purposes. In some cases, we may also disclose Personal Data to clients' affiliated entities, including parent, subsidiaries, and other related entities to meet these business purposes.

*Please note: we will not share your phone number or SMS consent information with any third parties for marketing purposes. If you have consented to receive text messages from GenSphire, you may receive text messages related to information about your application status, onboarding materials, other employment-related updates, or client assignments. Message and data rates may apply. All information you disclose will be subject to the third-party privacy policies and practices of such third parties.

Personal Data We Disclose for a Business Purpose

Service Providers. We may use third-party service providers to perform certain business services on behalf of us or the services and may disclose Personal Data to such service providers as needed for them to perform these business services. Service providers are only allowed to use, disclose or retain the Personal Data to provide these services and are prohibited from selling Personal Data. Business services provided include, but are not limited to, background check and employee eligibility providers, employee benefit and insurance providers, training platforms, time keeping and payroll providers, security and building access providers, healthcare providers, uniform companies, communications and video conference providers, internal social media platform provider, and other software and technology providers.

Internal Third Parties. We may disclose Personal Data to our parent company, subsidiaries and other related companies owned by or controlled by or under common ownership, who may use the Personal Data for the purposes described above.
Categories of Personal Data that have been disclosed for a business purpose in the past twelve months to service providers and internal third parties include:

Identifiers
Contact Information
Characteristics of protected classifications under California or federal law
Information about your job
Education information
Professional or employment related information and documents
Internet and other electronic network activity information
    Audio and visual information
    Marketing and Communications Data
    Data Voluntarily Submitted
Performance and disciplinary information
Information about your compensation and benefits
Family Information
Financial information
Health information
Union membership status
Termination and Post-Employment Information

Personal Data Sold or Shared. We do not sell any Personal Data. In the United States, we have shared information about your interaction with our website in the past twelve months with Google by allowing Google to place cookies and a Remarketing Code on our website for data analytics and to serve ads to you about our products and services as you browse the Internet. You can learn more about how Google collects and uses information from their website at: www.google.com/policies/privacy/partners/., if your browser supports it, you can turn on the Global Privacy Control (GPC) to opt-out of the "sharing" of your Personal Data. Learn more at the Global Privacy Control website. We do not have any actual knowledge of selling or sharing Personal Data of minors under 16 years of age.

Business Transactions. We may do business with third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. During the period leading up to and including the completion, if any, of a business transaction, your Personal Data may be collected, used or disclosed but such collection, use or disclosure will be restricted to purposes that relate to the business transaction. If a change happens to our business, then the new owners may use your Personal Data in the same way as set out in this Statement.

Legal Process. Subject to applicable law, we may disclose information about you (i) if we are required to do so by law, regulation or legal process, such as a subpoena; (ii) in response to

requests by government entities, such as law enforcement authorities; (iii) when we believe disclosure is necessary or appropriate to prevent physical, financial or other harm, injury or loss; or (iv) in connection with an investigation of suspected or actual unlawful activity.

Information You Provide To A Third Party. We may contract with third party service providers that operate their own websites and online platforms on which you will need to create an account ("Third-Party Sites"). GenSphire does not control any Third-Party Sites and is not responsible for any information they may collect. The information collection practices of a Third-Party Site are governed by its privacy Statement. It is your choice to enter any Third-Party Site. We recommend that you read its privacy Statement if you choose to do so.

HOW WE PROTECT THE PERSONAL DATA WE COLLECT

We have technical, administrative, and physical security measures in place designed to protect your Personal Data from unauthorized access or disclosure and improper use. For example, we use Transport Layer Security (TLS) encryption to protect the data collection forms on our website. In addition, we restrict access to your Personal Data to employees who need the Personal Data to perform a specific job (for example, a customer service representative). Employees with access to Personal Data are kept up-to-date on our security and privacy practices. It is important for you to protect against unauthorized access to your password and to your computer. Be sure to close your browser after you have completed your visit to the website or any of our online systems. Please note that despite our reasonable efforts, no security measure is ever perfect or impenetrable, so we cannot guarantee the security of your Personal Data.

REGION-SPECIFIC INFORMATION

1. a) California Privacy Rights

The California Consumer Privacy Act as amended ("CCPA") provides California residents with specific rights regarding their Personal Data. This section describes your CCPA rights and explains how to exercise those rights.

Right to Know: You have the right to know what Personal Data we have collected about you in the immediately preceding 12-month period, including the categories of Personal Data, the categories of sources from which the Personal Data is collected, the business or commercial purpose for collecting, selling, or sharing Personal Data, the categories of third parties to whom we have disclosed Personal Data, and the specific pieces of Personal Data we have collected. You may exercise this right no more than twice in any 12-month period.

Right to Delete: You have the right to request that we delete Personal Data that we collected from you and retained, subject to certain exceptions.

Right to Correct: You have the right to correct inaccurate Personal Data that we maintain about you.

Right to Opt-Out of the Sale/Sharing: You have the right to opt-out of the sale or sharing of their Personal Data by the business. We do not sell your Personal Data.

Right to Limit the Use or Disclosure of Sensitive Personal Information: You have the right to request that we limit the use and disclosure of sensitive Personal Information to specific

business purposes approved by the CCPA. Our use of Sensitive Personal Information is already limited to the approved business purposes identified above.

Right to Non-Discrimination: Unless permitted by applicable law, we will not discriminate against you for exercising any of your privacy rights under CCPA or applicable law, including by, but not limited to:

1. Denying you goods or services;
2. Charging you different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
3. Providing you a different level of quality of goods or services; or
4. Suggesting that you will receive a different price or rate for goods or services or a different level of quality of goods or services.

Exercising Your Rights

Requests can be submitted by contacting jobs@GenSphire.com. You can also opt out of sharing (having Personal Data transmitted through third-party cookies and pixels) by declining cookies when you first visit our website. Additionally, if your browser supports it, you can turn on the Global Privacy Control (GPC) to opt-out of the "sharing" of your Personal Data.

Only you, or a person that you authorize to act on your behalf, may make a verifiable consumer request related to your Personal Data.

Authorizing an Agent to Act on Your Behalf

Except where you have provided an agent with a Power of Attorney pursuant to Sections 4000 – 4465 of the California Probate Code, when using an authorized agent you must: (1) provide the agent with signed written permission clearly describing their authority to make a request on your behalf; (ii) verify your own identity; and (iii) directly confirm that you have provided the authorized agent permission to submit the request. We may deny a request from an authorized agent if the agent does not provide us with the signed written permission demonstrating that they have been authorized to act on your behalf.

Verifying Your Request

The verifiable consumer request initiated by you or your authorized agent must:

Include your full legal name, and email, which we will need to contact you in order to verify that you are the person about whom we collected Personal Data or an authorized representative.

Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with Personal Data if we cannot verify your identity or authority to make the request and confirm the Personal Data relates to you. Making a verifiable request does not require you to create an account with us. One of our representatives will contact you in order to verify your identity. You may need to provide additional information in order to verify your request. Depending on the nature of the request, we may require additional verification actions be taken, including but not limited to providing a signed declaration under penalty of perjury that you are the person whose Personal Data is the subject of the request.

We will only use this information to verify the requestor's identity or authority to make the request.

Exceptions.
These rights are not absolute and are subject to certain exceptions. For example, we cannot disclose or permit access to specific pieces of Personal Data if granting your request would present a certain level of risk to the security of the Personal Data at issue, your account with us, or the security of the website.
We may deny your deletion request if retaining the information is necessary for us or our service providers and/or contractors to:

Engage in employment related activities and take actions reasonably anticipated within the context of our employment relationship with you.
Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
Exercise a right provided for by law.
Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.).
Enable solely internal uses that are reasonably aligned with expectations based on your employment relationship with us.
Comply with a legal obligation.
Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Response Timing and Format
We endeavor to respond to a verifiable request within a reasonable number of months of its receipt. If we determine that the request warrants a fee, we will provide you with a cost estimate before completing your request.

1. b) Canada

The Company makes commercially reasonable efforts to keep your personal information complete, up-to-date and accurate. Should you wish to access, update, correct or delete your personal information or express any concerns regarding our use of your personal information, please contact our Privacy Officer at admin@GenSphire.com. We ask that you provide us with the name, address and email address that you previously provided to us, a brief description of under what circumstances you provided your personal information to the Company, and the purpose of your request. If you are unsure as to whether the Company is holding any personal information that belongs to you, you may also contact our Privacy Officer for confirmation.

The Company will make reasonable efforts to respond to your request as soon as practicable, or in any event, in compliance with applicable laws. In order to protect your privacy and security, the Company will take steps to verify your identity before granting access or making any changes to the personal information that we maintain.

GenSphire may transfer your Personal Data outside Canada to its affiliates, third party service providers, and potential employers with operations in other countries, which are subject to laws

of a foreign jurisdiction. GenSphire uses contractual or other means to provide a comparable level of protection while Personal Data is being processed by a third party. By accepting this Privacy Statement and providing us with your Personal Data you acknowledge and consent to your Personal Data being processed by third parties and being transferred, accessed and/or stored in countries outside Canada.

2. c) Quebec Residents

If you are a resident of Quebec, you have certain additional rights under applicable data protection laws. These may include the rights (i) to restrict dissemination of your personal information or to have your personal information de-indexed from search results (the right to be forgotten); (ii) to be informed when your personal information was used to render a decision based exclusively on automated processing and to request further information about the automated decision-making; and (iii) to data portability. If you have a request regarding these rights please contact our Privacy Officer at admin@GenSphire.com. We will consider and act upon any request in accordance with applicable data protection laws.

Changes to this boilerplate Statement

We may modify or update this Statement from time to time. We encourage you to revisit this page often to remain fully informed of our Statement, or you can contact us anytime to obtain the latest copy.

Questions about this boilerplate Statement

If you have any questions or concerns about this Statement, you can contact us by email at admin@GenSphire.com or jobs@GenSphire.com

Last Updated: April 1st 2025