PSI Services LLC
Job Applicant Privacy Notice

Effective Date: January 1, 2023

At PSI ("**we", "us"," our**"), we are committed to safeguarding your personal data and respecting your privacy. This Privacy Notice outlines how we collect and use the personal data of our job applicants (hereinafter referred to as "**you", "your", "individual**") during the application and recruitment process, in compliance with applicable **Data Protection Laws**, including the UK General Data Protection Regulation ("**UK GDPR**"), the California Privacy Rights Act ("**CPRA**"), and other data protection laws worldwide. These laws ensure that you are informed of your rights and our data handling practices.

This Privacy Notice supplements the information contained in PSI's Privacy Policy and applies to all individuals applying for employment with PSI Services LLC.

Information We Collect

Personal data, or personal information refers to any information that identifies or relates to you as an individual. This may include, but is not limited to, your name, contact details, employment history, education, identification numbers, and other information required during the application process. It does not include information where the identity has been removed (anonymous information).

We may collect, store, and process the following categories of information:

- **Personal details** such as full name, alias, address (including proof of address), date and place of birth, age, telephone number(s), email address, unique personal identifier, online identifier, Internet Protocol address, account name, social security number, national insurance number, driver's license number, passport number, photograph(s), or other similar information.

- **Work history**, including previous employers, positions, dates, responsibilities, and performance evaluations.

- **Education**, including professional qualifications, skills and/or memberships.

- **References** and remuneration information.

- **Financial information** such as bank account details for salary payments (if successful).

- **Results of pre-employment screening checks**, such as veteran or military status, credit history, and background check information.

- **Notes from interviews**, including psychometric tests or assessment results.
- **Video and audio recordings** of interviews, where permitted by law and with your consent.
- **Inferences drawn from other personal data**, such as profiles reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

In some circumstances, we may ask you to allow us to collect, store and process special and/or sensitive personal data. When doing so, we will provide you with information about the purpose of collection, and you may decide whether to give consent. If you do not provide sufficient information, we may not be able to process your application properly and meet our legal obligations. This type of information may include:

- **Information about your race or ethnicity, religious beliefs, sexual orientation and union membership.**
- **Information about your health**, including any medical condition and sickness records.
- **Criminal record checks**, where permitted by law.

Important Notice: Please note that not all of the personal data listed above may be collected during every application process. The specific information we collect may vary depending on the role and the nature of the application process.

Additionally, depending on applicable Data Protection Laws, sensitive personal data may include other categories, such as social security number, passport number, or driver's license number, as defined under laws like the California Privacy Rights Act (CPRA).

Purposes of Processing

We process personal and sensitive data during the application and recruitment process based on a lawful basis, which may vary depending on your location and applicable Data Protection Laws. Your personal data will only be processed where a lawful basis applies. This may include progressing your application, complying with legal or regulatory requirements, or managing our recruitment processes. Not all purposes will always apply to every individual.

In particular, the purposes are:

- **Contractual necessity**: We may process your personal data to take steps prior to entering a contract with you or to fulfill our contractual obligations once an employment contract is agreed upon.
- **Legal obligations**: In some cases, we must process personal data to ensure compliance with legal or regulatory requirements. For example, we are required to verify a successful applicant's eligibility to work in certain jurisdictions before employment can commence.

- **Legitimate interest**: PSI has a legitimate interest in processing personal data throughout the recruitment process and in maintaining records of that process. Processing your personal data helps us manage recruitment, assess your suitability for employment, and decide whether to offer you a position.

- **Consent**: PSI may process sensitive personal data, such as information related to race, ethnicity, disability status, or other factors, for the purposes of monitoring recruitment statistics and to comply with legal obligations relating to equality and diversity. In certain cases, we may collect information about disabilities to ensure reasonable adjustments are made during the recruitment process, in line with legal requirements.

- **Vital interests**: To comply with health and safety obligations.

- **Compliance with employment-related obligations**: we may also process personal data to fulfill obligations and exercise specific rights related to employment, social security, or social protection under applicable laws.

Please note that the specific processing activities and purposes may vary depending on the role you apply for and the applicable legal requirements in your location.

How is your Personal Data Collected?

We collect personal data about you through the application and recruitment process, either directly from you or sometimes from an employment agency or a background check provider. We may also collect additional information from third parties including former employers, credit reference agencies or other background check agencies. Additionally, we will collect additional personal data in the course of job-related activities if you are employed with us.

We will only request personal data that we believe is necessary for the application and recruitment process. You are not under any statutory or contractual obligation to provide personal data during this process. However, if you choose not to provide sufficient personal data, we may be unable to properly process your application or fulfill our obligations.

Disclosing Personal Data

We do not share or sell your personal data with third parties for their own marketing or business purposes.

We may disclose your personal data both internally, within PSI, and externally to third parties. When disclosing personal data to a third party, we enter into a contract that describes the purpose of processing and requires the recipient to keep that personal data confidential and handle it in accordance with Data Protection Laws.

For example, where required by law and with your consent, we may disclose your personal data to credit or criminal checking agencies; or to credit reference agencies to assist us with employment verification. Additionally, we may disclose your personal data to educational entities (e.g., universities, colleges) for the purpose of validating the information you have provided; and to other third parties such as HR and employee benefits providers, external advisors and governmental organizations.

For more information about the disclosure of personal data, please contact us at psi-dpo@psionline.com

Retention of Personal Data

We retain your personal data in accordance with our data retention policies. If your application for employment is unsuccessful, PSI will retain your data on file for up to 2 years for UK-based applications and up to 3 years for US-based applications, in compliance with legal and regulatory requirements, unless you choose to request its deletion.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your Human Resources file and retained in accordance with our data retention policies. In this case, our employee Privacy Notice will apply to you.

You may also be asked, when submitting your CV and personal data, whether you consent to have your details retained for consideration for other positions.

Your Legal Rights

Under applicable Data Protection Laws, which may include the UK GDPR, the CPRA, and other relevant Data Protection Laws, individuals have specific rights regarding their personal data. This section describes your data protection rights and explains how to exercise those rights.

Depending on your jurisdiction, the following rights under Data Protection Laws may apply to you in relation to your personal data:

- **The right to know**: You have the right to request information about our collection, use, and disclosure of your personal data. This privacy notice is designed to provide you with that information.

- **The right of access**: This allows you to receive a copy of the personal data we hold about you.

- **The right of rectification or correction**: This helps you to have any incomplete or inaccurate information we hold about you corrected.

- **The right of erasure or deletion**: This enables you to request that we delete or remove personal data where there is not a lawful basis for us continuing to process it.

- **The right to data portability**: This gives you the right to request the transfer of your personal data to another party.

- **The right to restrict processing**: You have the right to request that we limit or stop processing your personal data under certain conditions, such as when you contest its accuracy or object to its use.

- **The right to object**: You have the right to object to the processing of your personal data for specific purposes, such as direct marketing or when processing is based on legitimate interests. If you exercise this right, we must stop processing your information unless we have compelling legitimate grounds to continue

- **The right to withdraw consent**: In the limited circumstances where you have provided your consent for the collection and processing of your personal data for a specific purpose, you have the right to withdraw your consent at any time. To withdraw your consent, please contact us. Once we have received notification of your withdrawal, we will no longer process your information for the purposes you originally agreed to, unless we have another legitimate basis for doing so under the law.

- **The right to lodge a complaint**: You have the right to file a complaint with a relevant supervisory authority if you believe that your personal data is being processed in violation of applicable Data Protection Laws.

- **The right not to be subject to a decision based solely on automated processing**, including profiling, which produces legal effects concerning you. This enables that you are not unfairly treated by decisions made entirely through automated means.

- **The right to opt-out of the sale of personal data**, and to request information about whether we have sold your personal data in the past 12 months. As stated above, we do not sell your personal data.

- **The right to limit the use and disclosure of sensitive personal data:** You have the right to restrict how we use and disclose your sensitive personal data, such as information revealing racial or ethnic origin, health information, or other sensitive details.

If you wish to exercise any of your applicable rights, please submit a request to us through our Privacy Portal. We will not discriminate against you for exercising any of the rights under Data Protection Laws.

You will not have to pay a fee to access your personal data or to exercise any of the other rights under Data Protection Laws. Only you, or someone legally authorized to act on your behalf, may make a verifiable request. Your request must provide sufficient information that allows us to reasonably verify that you are the person about whom we collected personal data. As a security measure, we may need to request specific information from you to help us confirm your identity.

We try to respond to all legitimate requests within the time period specified under Data Protection Laws. Occasionally, it may take us longer than the specified time period if your request is particularly complex or you have made multiple requests. In such cases, we will notify you.

International Transfers

PSI may share your personal data within PSI for the purposes of processing your job application. We primarily store your information in the United States, the United Kingdom ("**UK"**), and the European Economic Area ("**EEA"**).

When transferring personal data, including outside the EEA, Switzerland, or the UK, PSI ensures that appropriate safeguards are in place. These include reliance on the EU-U.S. Data Privacy Framework (and its extensions for Switzerland and the UK) and the use of Standard Contractual Clauses in contracts with third parties. This ensures adequate protection when transferring personal data and compliance with GDPR and other applicable Data Protection Laws.

For more information about our Data Privacy Framework (DPF) certification, as we are self-certified, please see our DPF Notice. If you need further details on the safeguards we have in place. For additional details on the safeguards in place, you can contact us at psi-dpo@psionline.com.

Security Measures

We have implemented various electronic safeguards and managerial processes to protect your personal data during the job application process. These measures are designed to prevent unauthorized access or disclosure, maintain data integrity, and ensure the appropriate use of your information.

Our information security program adheres to industry best practices and guidance from sources such as the National Institute of Standards and Technology (NIST), Payment Card Industry (PCI) standards, the Centre for Internet Security (CIS), and the International Standards Organization (ISO), specifically ISO/IEC 27001:2012 (Security techniques — Information security management systems — Requirements).

Personal data related to job applications is stored on secure servers located in the United States, the United Kingdom (UK), and the European Economic Area (EEA). All applicant accounts are password-protected to prevent unauthorized access. Access to your personal data is limited to those with a legitimate business need. We ensure that all individuals handling your information follow our instructions and are bound by confidentiality obligations. We have established procedures to address any suspected breaches. If a breach occurs, we will notify you and any relevant regulatory authorities as required by Data Protection Laws.

While we take commercially reasonable steps to protect your personal data, no security measures can guarantee complete security. Data transmission over the internet carries inherent risks, and we cannot warrant the security of any information transmitted to us.

Changes to Our Privacy Notice

We reserve the right to amend this Privacy Notice at our discretion and at any time. When we make changes to this Privacy Notice, we will post the updated notice on the Website and update the notice's effective date. You should review this Notice periodically to keep up to date on our most current policies and practices.