The Walsh Group Privacy Policy

Effective date: 07/01/2005
Revision date: 01/01/2025

Introduction

This policy describes how the Company collects and uses candidate and employee data. It covers personal data collected by our website, applicant tracking system, onboarding system, and core human capital management systems. Our policy demonstrates our commitment and obligation to uphold privacy standards.

The Company does reserve the right to make changes to this Policy at any given time. This policy will provide information on:

- The information we collect
- How we collect the information
- What is considered personal information
- Compliance with local laws
- How we use your personal data
- How we share your personal data
- Security and Breach Notification
- Retention of data
- Reporting Violations

The Information We Collect

The Company collects personal information that is required to pursue its business operations and to comply with government reporting and disclosure requirements. We may collect different types of personal information from our applicants and/or employees based on their position, benefit elections, and driving authorization. Some examples of information we collect includes, but is not limited to:

Candidates:

- Individual Personal Information – legal name, date of birth, gender, ethnicity, home address, and social security card.
- Resume and application – which will include education, past employment information, and skills/abilities.
- Information automatically collected when visiting our website or affiliated websites, which may include cookies, sourcing information, third party tracking technologies, and server logs.

Pre-Hires and Employees:

- Individual Personal Information – legal name, date of birth, gender, ethnicity, home address, and social security card.

- Information automatically collected when visiting our website or affiliated websites, which may include cookies, sourcing information, third party tracking technologies, and server logs

In addition to what is collected above:

- Banking Information- personal bank, routing number, and account numbers.
- Dependent Information – legal name, date of birth, social security card, resident address.
- Medical Information – if a reasonable accommodation or leave of absence is requested, we may obtain information about past or present medical information.
- Driving Authorization Information – Driver's License number, expiration date, and state of issue.

How We Collect the Information

We may collect your information in a variety of ways:

- Employment application
- Forms that you complete at time of hire.
- Forms submitted through email, fax, interoffice mail, or through postal services.
- Information entered through our systems. As well as information gathered when visiting our website and associated sites.
- Documentation received from outside vendors, such as
    - Background Investigation
    - Benefit Enrollments
    - Motor Vehicle Reports

What is Considered Personal Information

We consider the following items to be protected personally identifiable information (Protected PII). This is any information that can be used to identify an individual. Examples include:
Direct Identifiers:

- Full Legal Name
- Social Security Number
- Passport Number
- Driver's License Number
- Financial Account Number
- Home Address and Telephone Number

Indirect Identifiers:

- Gender
- Race
- Date of Birth

Biometric Records:

- Photographic image, x-rays, fingerprints, retina scan, voice signature, facial geometry.

Information not included in protected personal information would be any information that can be lawfully obtained from public records, federal, state, or local government records or cannot be used on its own to identify, trace, or identify a person. This may include, but is not limited to: Device IDs, Cookies, browsing history, location information, and IP addresses.

Compliance with Local Laws

This policy is a general guide on how the Company processes personal data. As such, those that access our system(s) should be aware that data protection and privacy laws can vary in different jurisdictions where the Company operates and has applicants, employees, and others that may visit our website and associated sites. Where applicable laws are stricter than this Policy, the Company has or will adopt specific privacy practices in those locations to satisfy the stricter requirements.

How We Use Your Personal Data

Access to information gathered regarding our employees is limited to personnel who need the information to perform their job responsibilities. We maintain physical, electronic, and procedural safeguards that meet state and federal regulations. We continually update and improve our security standards, procedures, and technology to protect against unauthorized access to your confidential information. The Company uses personal data that is collected primarily for the purposes of managing its employment relationship with its employees, along with other legitimate business purposes. Such use includes, but is not limited to:

- Determining eligibility for hiring, including the verification of reference, qualifications, and criminal records (for certain purposes and permissible by law).
- Sourcing information to learn more about how our applicants find us.
- Administering payroll and benefits, processing employees' work-related claims (i.e. workers compensation), processing reasonable accommodations, and leave of absence requests.
- Establishing training and/or development requirements.
- Shipping and delivery of Company information to your home address.
- Establishing emergency contacts and responding to emergencies.
- Complying with application laws, implementing, or responding to court orders.
- Preventing or detecting fraud or other types of wrongdoing.
- Implementing and administering IT systems and information security, including authentication to access the Company systems and network.
- For other lawful or legitimate purposes, which are reasonably required for day-to-day operations.

How We Share Your Personal Data

The company does not sell employee personal data.

Information shared with outside vendors is submitted and received in a secure electronic manner which is consistent with security standards. We may share your personal data with those who need access to perform their duties, including but not limited to the following:

- Other Employees, i.e. Human Resources, Risk Management, etc.
- To our Service Providers acting on our behalf, i.e. Benefits, 401(k), etc.
- Government Reporting as required by law

The Company may be required by law enforcement, legal requests, owner requirements or judicial authorities to provide information about its employees to the appropriate authorities. The Company will comply with these requests.

In matters involving a danger to personal or public safety, the Company may voluntarily provide information to appropriate governmental authorities.

Security and Breach Notification

The Company maintains appropriate safeguards to protect personal data from accidental, unlawful, or unauthorized access. Our services providers are required to keep personal data confidential and secure.

The Company has a dedicated team responsible for monitoring and responding to security events, and it notifies applicable parties of security or privacy incidents and data breaches in accordance with its incident response procedures and applicable law.

Retention of Data

Unless a longer retention period is required by law, we will retain your personal data for as long as we have a legitimate business purpose/interest in that data. Generally, this means we will keep your personal data until the end of your employment with us, plus a reasonable period of time after your employment ends. This is so we can respond to any necessary employment inquiries regarding legal, tax, accounting or administrative matters or to provide you with ongoing benefits.

Reporting Violation

Employees are expected to report any suspected violation of this policy to their Supervisor, Business Group Leader, Human Resources Department, Legal Department, or The Walsh Group Hotline by phone 1-888-873-6086 or by email at hotline@walshgroup.com.

No adverse action or retaliation of any kind will be taken against an employee because he or she reports a suspected violation of this policy. Such reports shall be treated confidentially to the extent practical, consistent with the need to conduct a thorough investigation.

Employees must cooperate in company investigations related to a violation of this policy and failure to cooperate or providing false information may result in disciplinary action, up to and including, termination of employment.