Privacy Statement - Workers

Effective August 10, 2017

Quick Summary

Privacy Mission Statement

Sterling Talent Solutions is committed to the protection of individual privacy rights. We hold ourselves to the highest legal and ethical standard for compliance and strive to be a privacy champion in the human resources technology industry. We value the trust our clients, colleagues and suppliers place in us, and we work to maintain that trust by building privacy protection into everything we do.

Contents

1 Scope of application

This statement applies to the collection and processing of personal information, which means information about an identifiable individual (you), that Sterling Talent Solutions (Sterling, we or us) collects about current or former employees, job applicants, contractors, subcontractors, and employees of contractors or subcontractors (collectively referred to as workers).

Work product you create for Sterling is not your personal information and is generally outside the scope of this document. However, work product may be the personal information of another worker if it is about that worker, such as a performance appraisal.

2 What types of personal information do we collect and why do we collect it?

The table below outlines the purposes for collecting personal information, the general types of personal information we collect, and where we collect it from.

Figure 1: Purpose of collection and data types

Purpose for collection	Types of personal information collected	Source(s)
Worker identification and relationship management	Name, postal address, telephone number, email address, photograph, interests, other personal characteristics you choose to share*	You
Recruiting, selection and screening (both pre-employment and ongoing)	Skills, education history, employment history, date of birth*, place of birth*, address history, criminal, police and court records*, drug test results*, professional credentials, credit history, identity documents or numbers*, appearance on government watch or sanctions lists, professional sanctions, nationality*, citizenship or immigration status*, sex or gender*, referrals of friends and family, racial, ethnic, sexual or other minority status*, opinions about you	You, educational institutions, employers, police, courts, credit reporting agencies, drug testing labs, professional organizations, government agencies, other publicly available sources, references you provide
Attendance and accommodation management	Hours worked, reason for leave or tardiness*, medical information*, family information*, disability information*	You, medical professional, your family member or other representative
Benefits management and employee support	Medical information*, disability information*, marital status*, family information*, transportation records, vehicle information, charitable donation information, professional development and education information, personal concerns or problems*	You, medical professional, third-party benefits provider
Payroll and tax management	Identity documents*, date of birth*, government ID numbers*, loan information, wage garnishment information, banking information*, marital status, family information	You, courts, government agencies
Data security	Network use, login/logout records, IP address, login credentials, file access, internet browsing, email activities, chat activities, telephone calls, home office information, mobile device information, voicemails	You, remote monitoring

Purpose for collection	Types of personal information collected	Source(s)
Emergency management	Emergency contact information, medical information*	You
Feedback and improvement	Survey results, exit interviews, general feedback	You
Physical security, health and safety	Biometric data such as fingerprints or hand geometry*, contents of bags or storage spaces, photograph, entry and exit records, video and audio recordings, drug testing and medical screening*	You, CCTV cameras, physical inspections, medical professional, drug screening lab
Code of conduct enforcement, complaint resolution, protection of company brand and integrity	Activity in social media or news media, information about interpersonal relationships*, complaints or concerns, internal and external communications	You, social media, news media, complainants, internal or external investigations, remote monitoring
Performance and quality management	Computer and network activity, telephone calls, performance appraisals, training records	You, remote monitoring, your supervisor

**Items marked with an asterisk may be considered sensitive or may be subject to special protections in some places. They will not be collected in every case. They will not be collected where prohibited by law, and where permitted, they will only be collected and used in accordance with applicable law.*

Legal basis for collection and processing of personal information

We collect and process workers' personal information based on one or more of the following:

- We need to do so to fulfil an obligation under applicable law;
- We need to do so to fulfil an obligation under our contract with you;
- We need to do so in emergencies to protect your vital interests;
- We have a legitimate interest to do so and have taken your rights into consideration;
- We have your free and informed consent to do so.

Reuse of personal information for new purposes

We will not reuse personal information for a new purpose other than the original one(s) for which it was collected, unless one or more of the following is true:

- the new use is compatible with the original one, meaning you should reasonably expect it;
- we have notified you of the new use and given you an opportunity to object to it; or
- the new use is otherwise permitted or required by law.

3 When, why and how do we communicate personal information outside of Sterling?

We collect personal information for the following purposes. Select and expand the section for the activity that applies to you to understand that activity, the personal information we collect for it, how we use that personal information, and our legal basis for doing so.

To conduct background checks and otherwise gather information about you

Background checks, both before and during your relationship with us, require us to find or validate personal information with third party sources. To do so, we need to provide your personal information to allow the third party to find records about you. We generally provide the information that is required by the third party in the format and through the transmission method of the third party's choosing. This may involve transmitting information through a web site, phone call, email, fax, letter or in person.

To comply with our obligations as an employer

We may need to provide information about you to outside parties, such as government agencies, to comply with legal obligations under tax, labor or other laws. For more information about our legal obligations in your situation, speak with the HR team.

To engage service providers

While most of our work is done by our employees or authorized personnel who access personal information directly from our systems and whose activities are under our direct control, we use third-party service providers for certain specialized tasks. These tasks include storage of data, information technology support, and provision of benefits.

It would be impractical to list all service providers here, so we have listed types of service providers instead of individuals or organizations. To understand which service providers may receive your personal information, contact the HR or Privacy teams.

The table below lists the types of service providers we use, the purposes for which we use them and the types of personal information we may transfer to them. This table may be updated from time to time to meet new or evolving business requirements.

Figure 2: Service providers

Service provider	Types of information	Purposes for transfer
Payroll providers	Identifying information, financial information, hours worked, government-issued identifying numbers and other payroll- and tax-related information	Ensure wage payment
Data storage and delivery providers, including data centers/cloud providers, applicant tracking systems, recruiting systems, human resources information systems and others	All personal information in our custody	Secure data storage and delivery
IT support services	Personal information in our custody with which we require technical support	Technical support
Background screening and consumer reporting companies, including court runners, drug testing labs, police departments, translation agencies and credit bureaus.	Personal information required to complete background checks	Background screening
Benefits providers, including healthcare providers, financial institutions and others	Identifying information, health information, information about family members, financial information, and	Provision of benefits, including health plans, retirement plans, and

	other information required to provide benefits	support services

In exceptional circumstances

We may be asked to communicate personal information to law enforcement agencies, national security agencies, courts or other public bodies in any jurisdiction where we are subject to the law, regardless of where personal information is stored. If we receive a production order, warrant, subpoena or other enforceable demand, we will comply as required by law. If we receive a request to provide information voluntarily, we will consider your interests, our business interests, the interests of our clients, public safety implications and our legal obligations prior to deciding whether to communicate personal information.

We may proactively communicate personal information to law enforcement or other third parties if necessary to investigate or report a violation of the law or a contractual agreement, or if otherwise appropriate and permitted by law.

4 How do we ensure your personal information is accurate?

Much of the personal information we collect comes directly from you, in which case you are in control of its accuracy. You are encouraged to update your personal information regularly to ensure it is accurate and up to date. Information that is found to be inaccurate, either through our own audits or following your request for correction, is updated.

5 Do we engage in automated decision-making, profiling, or research using personal information?

We do not make automated decisions about you, nor do we attempt to analyze or predict your behavior, preferences, interests, health or other personal characteristics. We only conduct research using personal information that is explicitly collected for that purpose, such as demographic information and surveys.

6 How long do we keep personal information?

We keep personal information as long as we need it to fulfill our obligations. This is dependent on why we collected the information in the first place. Once we no longer need it, it is deleted or anonymized.

Most personal information is retained for as long as you perform work for us and a certain period afterwards. Certain information must be kept to comply with legal obligations under local employment and tax laws. For information about how long your personal information will be retained, contact the HR or Privacy teams.

7 Do we transfer personal information between countries?

Yes. We store and process personal information in Canada, India, the Philippines, the United Kingdom and the United States. We occasionally also use service providers in various other countries, usually to collect or translate information from that service provider's country or region that we require to provide services.

If your personal information is subject to European Union (EU) or Swiss law, it may be transferred outside of the EU or Switzerland based on one or more of the following legal mechanisms:

- Relevant authorities have issued a decision that personal information will benefit from an adequate level of protection in the country to which it is transferred. This is the case for Canada and, under the Privacy Shield Framework and the U.S.-Swiss Safe Harbor Framework, the United States. This is not the case for India or the Philippines.
- We have signed contractual clauses within our corporate group or with a third-party vendor that are deemed by the relevant authority to ensure adequate protection of personal information.
- You have provided your free and informed consent for us to transfer data outside of the EU or Switzerland.

In all cases, we ensure that appropriate safeguards are in place to ensure the protection of your personal information. For more information about these safeguards, please contact the Privacy team.

8 Do we participate in the Privacy Shield Framework and the U.S.-Swiss Safe Harbor Framework?

Yes. Sterling Infosystems Inc. and its U.S. affiliates and subsidiaries operating under the brand name of Sterling Talent Solutions (listed below under "Privacy Shield Covered Entities") comply with the EU-U.S. Privacy Shield Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal information transferred from the EU and Switzerland to the United States. Sterling has certified to the Department of Commerce that it adheres to the Privacy Shield Principles and the Safe Harbor Principles. Sterling remains responsible for personal information that is communicated to third parties for processing as described in Section 4 ("When, why and how do we communicate personal information outside of Sterling?). If there is any conflict between the terms in this statement and the Privacy Shield Principles or the Safe Harbor Principles, the Privacy Shield Principles and the Safe Harbor Principles will prevail. To learn more about the Privacy Shield and U.S.-Swiss Safe Harbor programs, and to view our certification, please visit http://export.gov/safeharbor and https://www.privacyshield.gov. The Federal Trade Commission has jurisdiction over Sterling's compliance with Safe Harbor and Privacy Shield.

8.1 Privacy Shield Covered Entities

- Abso, Inc.
- American Background Information Services, Inc.
- Bishops Services, Inc.
- Data Quick Direct, Inc.
- EmployeeScreen IQ, Inc.
- Screening International LLC
- Sterling Credit Screening, Inc.
- Sterling Infosystems Ohio, Inc.
- Sterling Protective Systems, Inc.
- Talentwise, Inc.
- The Premier Company, dba Tandem Select

- Unisource Screening & Information, Inc.
- Verified Person, Inc.

9 How do we protect personal information?

We have advanced security measures in place to secure and protect your personal information, such as internal and external firewalls, monitoring and alert systems to prevent and detect intrusion attempts, and 128-bit encryption of data both in transit and at rest. Our servers are located within a securely managed infrastructure, and undergo multiple reviews by independent auditors. Our employees access data through secure virtual desktop interfaces and our online interfaces are encrypted, password protected and monitored.

We employ equally rigorous physical security policies to prevent physical access to our premises. Our servers and offices, including personal information in hard copy form, are kept in access-controlled and monitored environments.

All of our employees have been carefully screened and undergone thorough security and privacy training. We restrict access to your personal information to individuals who need it to perform their work functions. Our human resources, facilities, information technology, finance, legal and quality teams, as well as people managers and executive leadership, may have regular access to your personal information and employees in other departments may access it occasionally as required to manage our relationship with you and fulfill our legal obligations.

We also enter into contractual agreements with service providers with which we may need to share your personal information, which require them to protect your personal information to the same level as we do, and allow us to audit their compliance with those obligations.

10 How can you choose how and whether we collect and use your personal information?

In some cases, providing your personal information is mandatory. For example, this is the case when we are required by law to collect the personal information from our workers (such as for tax or workers' compensation purposes), when the collection is necessary to fulfill our contract with you (such as for payroll purposes), and when we have determined that the collection is in our legitimate interest and is done in accordance with your rights (such as for background screening).

In other cases, providing your personal information is voluntary. If you choose not to provide your personal information in these cases, you may not be able to receive certain optional benefits.

To understand whether it is mandatory or optional to provide your personal information, and the consequences of choosing not to provide it, speak to the department requesting the personal information or the HR or Privacy teams.

Whenever our legal basis for collecting and using personal information is your consent, you can withdraw or modify your consent for future collection or use of your personal information at any time, and we will explain the consequences of doing so.

If we use your personal information for sales or marketing purposes, you can ask us to stop at any time and we will do so.

11 How can you access or correct your personal information, request that it be deleted, or ask for it to be transferred to another organization?

At any time, you can request access to your personal information, request that any inaccuracies be corrected, and request that comments or explanations be added to records about you.

You can also ask about:

- whether and why we have your personal information;
- how we got your personal information;
- what we have done with your personal information;
- to whom we have communicated your personal information;
- where your personal information has been stored, processed or transferred;
- how long we will retain your personal information, or how that retention period will be determined; and
- the safeguards in place to protect your information when it is transferred to third parties or third countries.

Finally, you can ask us not to collect or use your personal information for certain purposes, you can ask us to delete your personal information, or you can ask us to provide your personal information to a third party.

Depending on which laws apply to your personal information, we may only be able to do some of these things for you. If you request one of these things and we refuse to do it, we will explain your legal rights, the reason for our refusal and any recourse you may have.

12 How can you make a complaint about how we have handled your personal information or responded to a request to exercise your rights?

We commit to investigating and resolving complaints about our collection or use of your personal information. To make a complaint, contact the HR or Privacy teams.

For European Union residents

If you are in the EU, you should contact our UK office to resolve your complaint, regardless of which of our companies the complaint is about. If you are not satisfied with our resolution of your complaint, you may complain to the Information Commissioner's Office. We commit to cooperating with the panel established by the EU data protection authorities (DPAs) and comply with the advice given by the panel with regard to personal information transferred from the EU. For the purposes of the Privacy Shield, we are subject to the investigatory and enforcement powers of the Federal Trade Commission. In some conditions, you may be able to invoke binding arbitration to resolve your complaint where your data has been transferred to and processed in the United States.

For United States residents

If you are not satisfied with our resolution of your complaint, you can make a privacy complaint to the Federal Trade Commission or you can make a consumer reporting complaint to the Consumer Financial Protection Bureau.

For Canadian residents

If you are not satisfied with our resolution of your complaint, you may be able to make a complaint to one of the following regulatory agencies. Upon resolution of your complaint, we will let you know which of these, if any, may apply to your situation.

- Office of the Privacy Commissioner of Canada
- Office of the Information and Privacy Commissioner of Alberta
- Office of the Information and Privacy Commissioner for British Columbia
- Commission d'accès à l'information du Québec

13 Contact Information

United States

1 State Street Plaza
New York, NY 10004 USA
privacy@sterlingts.com
1-800-899-2272

Canada

Suite 200-19433 96th Avenue
Surrey, BC V4N 4C4 CANADA
privacy@sterlingts.com
1-800-455-5671

United Kingdom

8th Floor, Alexandra House
1 Alexandra Road
Swansea SA1 5ED UK
privacy@sterlingts.com
+44 (0)1792 478838
Information Commissioner's Office Registration Number: Z9745943

14 Glossary

Anonymized means that sufficient information has been removed from personal information so that it can no longer be associated with an identifiable individual.

Individual or you means the individual that personal information is about.

Personal information means information about an identifiable individual.

Processing, handling or use means anything we do with personal information.

Profiling means automated use of your personal information to analyze or predict things like your performance at work, creditworthiness, reliability and conduct.

Sterling Talent Solutions, Sterling, we or us means Sterling Infosystems, Inc. and all of the subsidiaries listed in the Contact Information section.

Service provider means a company engaged to process personal information on behalf of another company.

Third party means a person or organization that is neither you nor us.

Worker means *a current or former employee, job applicant, contractor, subcontractor, or employee of a contractor or subcontractor.*

Version history

Version History			
1.0	31 January 2017	M. Sward	First version of policy
1.1	28 March 2017	M. Sward	Updates to reflect Privacy Shield requirements
1.2	10 August 2017	M. Sward	Addition of quick summary, minor stylistic updates, addition of categories of employees who have access.