

## **STERLING TESTING SYSTEMS, INC. DATA PRIVACY POLICY**

Sterling InfoSystems Inc. d/b/a Sterling Testing Systems ("Sterling") respects individual privacy and values the confidence of its Clients, employees, vendors, consumers, business partners and others. Sterling strives to collect, use and disclose Personal Data in a manner consistent with the laws of the countries in which it does business, and has a tradition of upholding the highest ethical standards in its business practices. Sterling abides by the *Safe Harbor Principles* developed by the U.S. Department of Commerce and the European Commission and the Frequently Asked Questions ("FAQs") issued by the Department of Commerce on July 21, 2000. This *Safe Harbor Privacy Policy* (the "Policy") sets forth the privacy principles that Sterling follows with respect to transfers of Personal Data anywhere in the world, including transfers from the European Economic Area (EEA) (which includes the twenty-seven member states of the European Union (EU) plus Iceland, Liechtenstein and Norway) to the United States.

### **I. SAFE HARBOR**

The United States Department of Commerce and the European Commission have agreed on a set of data protection principles and frequently asked questions (the "*Safe Harbor Principles*") to enable U.S. companies to satisfy the requirement under European Union law that an adequate level of protection is given to Personal Data transferred from the EU to the United States. The EEA also has recognized the U.S. Safe Harbor as providing an adequate level of data protection (OJ L 45, 15.2.2001, p.47). Consistent with its commitment to protect Personal Data privacy, Sterling adheres to the *Safe Harbor Principles*.

Sterling has a Vice President of Compliance who assists in ensuring compliance with this Policy and data security issues. Sterling educates its employees concerning compliance with this Policy and has self-assessment procedures in place to assure compliance. Sterling's Vice President of Compliance Joe Rotondo and its external legal advisors are available to any of its valued employees, Clients, vendors, business partners or others who may have questions concerning this Policy or data security practices. Relevant contact information is provided herein.

### **II. SCOPE**

This Policy applies to all Personal Data received by Sterling in any format including electronic, paper or verbal.

Sterling collects and processes Personal Data concerning current and former employees of Sterling and their respective family members, as well as applicants for employment at Sterling through its Internet websites, its intranet site, electronic mail and manually. Sterling is the sole owner of information it collects from current and former employees, applicants for employment, Clients, vendors and others. Sterling will not sell or share this information with third parties in ways different than what is disclosed in this Privacy Policy. On a global basis, Sterling will, and will cause its affiliates to, establish and maintain business procedures that are consistent with this Policy.

Sterling collects Personal Data of its employees and/or job applicants for, among other things, legitimate human resource business reasons such as payroll administration; filling employment positions; administration and operations of its benefit programs; meeting governmental reporting requirements; security, health and safety management; performance management; company network access; and authentication. Sterling does not request or gather information regarding political opinions, religion, philosophy or sexual preference. To the extent Sterling maintains information on an individual's medical health or ethnicity (as legally required), Sterling will protect, secure and use that information in a manner consistent with this Policy and applicable law.

Through its service to Company Clients to conduct background and criminal record checks, drug testing, and employment verification, Sterling also collects and processes Personal Data of individuals who apply for employment at Sterling's Clients ("Client-employees" and "Client-employee Personal Data"). Sterling will conduct Client-services in accordance with the notice given to and/or the consent obtained from Client-employees. Sterling will not sell or share Client-employee Personal Data to third parties other than the Client on whose behalf the Personal Data was collected.

Personal Data collected by Sterling from prospective Clients, consumers, vendors, business partners and others. Sterling collects Personal Data for, among other things, legitimate business reasons such as Client service; product, warranty and claims administration; meeting governmental reporting and records requirements; maintenance of accurate accounts payable and receivable records; internal marketing research; safety and performance management; financial and sales data; and contact information. All Personal Data collected by Sterling will be used for legitimate business purposes consistent with this Policy.

Personal Data and Client-Employee Personal Data collected by Sterling are maintained at a secured data center located in the United States.

### **III. DEFINITIONS**

For purposes of this Policy, the following definitions shall apply:

"*Agent*" means any third party that uses Personal Data provided by Sterling to perform tasks on behalf of or at the instruction of Sterling.

"*Client-employee*" means a person who applied for employment at a potential employer and/or a person working for an employer which employer requested Sterling's Consumer Services regarding such a person.

"*Client-employee Personal Data*" means Personal Data of a Client-employee that Sterling collected and processed as part of its Client Services.

“*Client-Services*” means employment screening services, which include back ground checks involving criminal records searches, credit checks, vehicle motor which search, social security trace reports, personal identification, number trace reports, employment verifications, education record verifications and/or drug testing, where such background checks are permissible by law, which services Sterling render at the request of a Client of the Company.

"*Personal Data*" means any information or set of information that identifies or could be used by or on behalf of Sterling to identify an individual. Personal Data does not include information that is encoded or anonymized, or publicly available information that has not been combined with non-public Personal Data.

"*Sensitive Personal Data*" means Personal Data that reveals race, ethnic origin, trade union membership, or that concerns health. In addition, Sterling will treat as sensitive Personal Data any information received from a third party where that third party treats and identifies the information as sensitive.

"*Sterling*" means Sterling InfoSystems Inc., its predecessors, successors, subsidiaries, divisions and groups.

#### **IV. PRIVACY PRINCIPLES**

The privacy principles in this Policy are based on the seven *Safe Harbor Principles*.

1. NOTICE: Where Sterling collects Personal Data directly from individuals applying for employment at Sterling, it will inform them about the purposes for which it collects and uses Personal Data about them, the types of non-agent third parties to which Sterling discloses that information, if any, and the choices and means, if any, Sterling offers individuals for limiting the use and disclosure of their Personal Data. Notice will be provided in clear and conspicuous language when individuals are first asked to provide Personal Data to Sterling, or as soon as practicable thereafter, and in any event before Sterling uses the information for a purpose other than that for which it was originally collected. Sterling may disclose Personal Data if required to do so by law or to protect and defend the rights or property of Sterling. Sterling will collect Client-employee Personal Data only in accordance with the notice to and consent given by the Client-employee.
2. CHOICE: Sterling will offer individuals the opportunity to choose (opt-out) whether their Personal Data is (a) to be disclosed to a non-agent third party, or (b) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

For Sensitive Personal Data, Sterling will give individuals who apply for employment at Sterling the opportunity to affirmatively and explicitly (opt-in) consent to the disclosure of the information to a non-agent third party or the use of the information for a purpose other than the purpose for which it was originally collected or

subsequently authorized by the individual. Sterling collects sensitive Personal Data on Client-employees only pursuant the person's express consent.

Sterling will provide individuals with reasonable mechanisms to exercise their choices should requisite circumstances arise.

3. **DATA INTEGRITY:** Sterling will use Personal Data only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. Sterling will take reasonable steps to ensure that Personal Data is relevant to its intended use, accurate, complete and current.
4. **TRANSFERS TO AGENTS:** Sterling will obtain assurances from its Agents that they will safeguard Personal Data consistently with this Policy. Examples of appropriate assurances that may be provided by Agents include: a contract obligating the Agent to provide at least the same level of protection as is required by the relevant *Safe Harbor Principles*, being subject to EU Directive 95/46/EC (the *EU Data Protection Directive*), Safe Harbor certification by the Agent, or being subject to another European Commission adequacy finding (e.g., companies located in Switzerland). Where Sterling has knowledge that an Agent is using or disclosing Personal Data in a manner contrary to this Policy, Sterling will take reasonable steps to prevent or stop the use or disclosure. Sterling holds its Agents accountable for maintaining the trust our employees and Clients place in the company.
5. **ACCESS AND CORRECTION:** Upon request, Sterling will grant individuals reasonable access to Personal Data that it holds about them. In addition, Sterling will take reasonable steps to permit individuals to correct, amend or delete information that is demonstrated to be inaccurate or incomplete. Any employees of Sterling who desire to review or update their Personal Data can do so by contacting their local Human Resources Representative. Client-employees must contact their employer and/or the company to whom they gave consent to conduct the Client Services.
6. **SECURITY:** Sterling will take reasonable precautions to protect Personal Data in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction. Sterling protects data in many ways. Physical security is designed to prevent unauthorized access to database equipment and hard copies of sensitive Personal Data. Electronic security measures continuously monitor access to our servers and provide protection from hacking or other unauthorized access from remote locations. This protection includes the use of firewalls, restricted access and encryption technology. Sterling limits access to Personal Data and data to those persons in Sterling's organization, or as agents of Sterling, that have a specific business purpose for maintaining and processing such Personal Data. Individuals who have been granted access to Personal Data are aware of their responsibilities to protect the security, confidentiality and integrity of that information and have been provided training and instruction on how to do so. Sterling will disclose Client-employee Personal Data only to the Client who requested the Client Services and in

accordance with the Notice provided by the Client to the Client employee and/or the consent given by the Client-employee.

7. ENFORCEMENT: Sterling will conduct compliance audits of its relevant privacy practices to verify adherence to this Policy and the U.S. Department of Commerce *Safe Harbor Principles*. Any employee that Sterling determines is in violation of this Policy will be subject to disciplinary action up to and including termination of employment.

## **V. DISPUTE RESOLUTION**

Any questions or concerns regarding the use or disclosure of Personal Data should be directed to the Sterling Privacy Office at the address given below. Sterling will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data in accordance with the principles contained in this Policy. For complaints that cannot be resolved between Sterling and the complainant, Sterling has agreed to participate in the dispute resolution procedures of the panel established by the European data protection authorities to resolve disputes pursuant to the *Safe Harbor Principles*.

## **VI. INTERNET PRIVACY**

Sterling views the Internet, intranets and the use of other technologies as valuable tools for communicating and interacting with consumers, employees, vendors, business partners and others. Sterling recognizes the importance of maintaining the privacy of Personal Data collected through websites that it operates. Sterling's sole purpose for operating its websites is to provide information concerning products and services to the public. In general, visitors can reach Sterling on the Web without revealing any Personal Data. Visitors on the Web may elect to voluntarily provide Personal Data via Sterling websites but are not required to do so. Sterling collects information from visitors to the websites who voluntarily provide Personal Data by filling out and submitting online questionnaires concerning feedback on the website, requesting information on products or services, or seeking employment. The Personal Data voluntarily provided by website users is contact information limited to the user's name, home and/or business address, phone numbers and email address. Sterling collects this information so it may answer questions and forward requested information. Sterling does not sell or share this information with non-agent third parties.

Sterling may also collect anonymous information concerning website users through the use of "cookies" in order to provide better Client service. "Cookies" are small files that websites place on users' computers to identify the user and enhance the website experience. None of this information is reviewed at an individual level. Visitors may set their browsers to provide notice before they receive a cookie, giving the opportunity to decide whether to accept the cookie. Visitors can also set their browsers to turn off cookies. If visitors do so, however, some areas of Sterling websites may not function properly.

None, of Sterling's websites are directed toward children. Nevertheless, Sterling is committed to complying with applicable laws and requirements, such as the United States' *Children's Online Privacy Protection Act* ("COPPA").

Sterling website users have the option to request that Sterling not use information previously provided, correct information previously provided, or remove information previously provided to Sterling. Those that would like to correct or suppress information they have provided to Sterling should forward such inquiries to:

Sterling InfoSystems Inc.  
249 West 17<sup>th</sup> Street, Floor 6  
New York, New York 10011  
Tel: +1(212) 736-5100  
Attention: Joe Rotondo, Vice President of Compliance

The inquiries should include the individual's name, address, and other relevant contact information (phone number, email address). Sterling will use all reasonable efforts to honor such requests as quickly as possible.

Sterling websites may contain links to other "non-Sterling" websites. Sterling assumes no responsibility for the content or the privacy policies and practices on those websites. Sterling encourages all users to read the privacy statements of those sites; their privacy practices may differ from those of Sterling.

## **VII. CHANGES TO THIS SAFE HARBOR PRIVACY POLICY**

The practices described in this Policy are current Personal Data protection policies as of February 28, 2007. Sterling reserves the right to modify or amend this Policy at any time consistent with the requirements of the *Safe Harbor Principles*. Appropriate public notice will be given concerning such amendments.