

TSI INCORPORATED EU EMPLOYEE DATA PRIVACY POLICY

PURPOSE:

To set forth the policy of TSI Incorporated (“TSI”) in regard to its compliance with the Safe Harbor Principles of the U.S. Department of Commerce for the protection of Employee Data transferred from TSI’s subsidiaries and locations in the European Union (“EU”)¹ to the United States (“US”) as required by the EU Directive on Data Protection.

SCOPE:

This Employee Data Privacy Policy (“Policy”) applies to TSI in its processing of Employee Data received from its subsidiaries in the EU.

POLICY:

TSI is the US based parent company of companies in many locations around the world, including the EU. The EU’s comprehensive privacy legislation, the Directive on Data Protection (the “Directive”), requires that transfers of Employee Data take place only (1) where a relevant basis exists upon which a transfer may be made, or (2) to non-EU countries that provide “adequate” protection for the Employee Data. Nonetheless, the US Department of Commerce in consultation with the EU authorities has developed a “safe harbor” framework to assist US companies in complying with the Directive. The safe harbor framework consists of seven “Safe Harbor Principles” with which TSI must comply if it wishes to self-certify under the Department’s safe harbor. Materials concerning the Safe Harbor Principles can be found online at www.export.gov/safeharbor. This policy sets forth TSI’s procedures for complying with the Safe Harbor Principles in regard to Employee Data transferred from EU subsidiaries and locations.

This Policy shall be communicated to all employees of TSI’s EU subsidiaries and to all US employees who process or otherwise have access to the “Employee Data” discussed below.

Compliance with this Policy is mandatory, and any employee failing to comply will be subject to disciplinary action, up to and including termination of employment.

PROCEDURES:

1. Notice From time to time, TSI receives personal Employee Data regarding employees of its EU subsidiaries for the purposes of (a) general employment purposes including providing compensation benefits and related services, keeping updated organizational information, making employment-related decisions, and employee training, (b) facilitating company business by publishing email, phone, and identification information, and (c) processing and

¹ TSI Instruments, Ltd., TSI GmbH, TSI AB, TSI France, Inc.

investigating reports under TSI's various compliance programs. This Employee Data could include one or more of the following: name, address, job title and other job information, location, compensation information, identification numbers, employment history, copies of employment agreements, information concerning disciplinary issues, or information about actions or inaction relative to a legal requirement or other legal issue under the company's compliance responsibilities.

Such Employee Data is transferred only to third parties acting as agents of TSI for the purposes described above. In no case does TSI transfer Employee Data for any purpose not compatible with these purposes unless it first notifies the employee involved. In addition, except in limited and permissible circumstances, TSI does not transfer Employee Data deemed "sensitive" under the Directive to any third party. Examples of the circumstance under which such sensitive Employee Data might be transferred include (a) the transfer is in the vital interest of the employee or another person; (b) it is necessary for the establishment of legal claims or defenses; (c) it is required to provide medical care or diagnosis; (d) it is necessary to carry out TSI's obligations in the field of employment law; or (e) it is expressly permitted by an employee for a specific purpose.

Any employee of TSI's EU subsidiaries may contact TSI's Corporate Counsel or Vice President Human Resources with complaints regarding TSI's processing of Employee Data, or to "opt out" of the transfer of Employee Data as described in Section 2 below. The contact information for the Corporate Counsel and Vice President Human Resources is:

Corporate Counsel: Floyd Grabiell, 651-490-2774, floyd.grabiell@tsi.com
VP Human Resources: Brenda Rivera, 651-490-2731, brenda.rivera@tsi.com

2. Choice Any employee whose Employee Data is to be transferred to third parties as described in the Policy may choose not to have the Employee Data transferred. The employee must communicate his or her desire to opt out by contacting the persons named above. An employee exercising the right to "opt out" should be aware that by doing so, he or she may lose access to compensation services or related services, the employee may be excluded from relevant organizational charts or other Employee Databases, and/or TSI or its agents may be unable to provide required training, or the employee may be prevented by the lack of access from performing the duties of his or her position. An employee may not opt out of the transfer of Employee Data to a third party for the purpose of meeting applicable legal requirements or permitting the legitimate interests of TSI in making promotions, appointments, or other employment decisions.

3. Onward transfer In addition to the limitations of the transfer of Employee Data discussed above, TSI's transfers Employee Data only to third parties who

have agreed in writing to provide at least the same level of privacy protection for Employee Data as is required under the Directive or Safe Harbor Principles, or who agree to adhere to the same. Exceptions to this limitation include where an employee has given express permission to the transfer of his or her Employee Data to the third party, or where the transfer is necessary for the purpose of meeting an applicable legal requirement.

4. Security TSI takes reasonable precautions to protect Employee Data from loss, misuse, or unauthorized access, disclosure, alteration, or destruction. Employee Data is maintained in secure electronic and manual files at TSI, and access to the files is limited to TSI employees for whom access is necessary to properly process the Employee Data consistent with the stated purposes. When it is necessary to transfer Employee Data to third parties, the transfer is accomplished by methods designed to reasonably reduce the risk that the Employee Data is compromised. TSI maintains Employee Data in accord with its document retention practices, and only for so long as is necessary, after which the Employee Data is destroyed, deleted, or returned. TSI authorized employees are trained periodically on this Employee Data Privacy Policy, with emphasis on the need to maintain privacy and secrecy of the information, as well as the potential disciplinary consequences of failure to follow the policy.

5. Data Integrity TSI headquarters personnel coordinate closely with personnel from TSI's EU subsidiaries to ensure that Employee Data is relevant, up-to-date, accurate, complete, and reliable for its intended use.

6. Access An employee whose Employee Data is processed by TSI may request access to his or her Employee Data as processed for the purpose of correcting, amending, or deleting incorrect or inaccurate data. TSI may deny access where the burden or expense of providing access would be disproportionate to the risks to the requesting employee's privacy or where the rights of persons other than the requesting employee would be violated.

7. Enforcement

a. Recourse and remedies EU employees whose Employee Data is processed by TSI should report any complaints about such processing to the TSI Corporate Counsel or Vice President Human Resources as noted in Section 1 above. TSI will investigate the complaint and work toward its resolution. If the complaint is not resolved through the internal process, employees forward the complaint for arbitration under the rules and procedures of the International Centre for Dispute Resolution, www.icdr.org, a division of the American Arbitration Association.

b. Verification To verify compliance with the Safe Harbor Principles, TSI through its internal audit process periodically (not less than once per year) conducts a self assessment to ensure that (a) this EU Employee Data Privacy

Policy is accurate, comprehensive, prominently displayed, completely implemented and accessible, and conforms to the Safe Harbor Principles; (b) employees are informed of the internal arrangements for handling complaints and the mechanisms through which they may pursue complaints (see Section 7a above); (c) notifying third parties who receive Employee Data of the conditions of this Policy; and (d) TSI has in place procedures for training the appropriate employees on the implementation of this Policy and disciplining those who fail to comply.

8. Safe Harbor Provision TSI, Inc. complies with the U.S.-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. TSI has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view TSI's certification, please visit <http://www.export.gov/safeharbor/>