



Policy on Data Protection and Privacy of Personal Information

Scope

This policy applies to employees of Worldwide TechServices, LLC and its subsidiaries ("WWTS"). From time to time this policy may be supplemented by communications from Information Technology ("IT"), HR ("HR") and/ or the Legal Department. All supervisors are responsible for enforcing this policy. Employees are expected to be familiar with and comply with all such statements of policy in this area. Failure to do so may result in disciplinary action up to and including termination.

Intent

This policy's purpose is to inform employees of the principles under which WWTS processes personal information received from countries belonging to the European Union ("EU") or Switzerland. This policy complies with the U.S. Department of Commerce Safe Harbor Frameworks, which have been approved by the EU and Switzerland as an adequate way for WWTS to demonstrate that it complies with protections outlined in the EU Directive on Data Protection and the Swiss Federal Act on Data Protection.

Affirmation

WWTS complies with the U.S.-EU Safe Harbor 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 from European Union member countries and Switzerland. WWTS 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 WWTS's certification, please visit <http://www.export.gov/safeharbor/>

Policy and Procedure

Definitions

"Personal data" and "personal information" are data about an identified or identifiable individual, received by WWTS in the U.S. from the EU or Switzerland, and recorded in any form.

A "data subject" is the individual who is the subject of personal data or information.

"Processing" means any online and offline processing and includes such activities as copying, filing, and inputting personal information into a database.



"Sensitive data" is data that pertains to racial or ethnic origins, political or religious beliefs, or health or sex life. Sensitive data may not be processed unless the individual has given explicit consent.

The Safe Harbor Privacy Principles

In processing personal data, WWTS complies with the following Safe Harbor Privacy Principles. Adherence to the principles may be limited in certain cases to the extent necessarily to meet national security, public interest, or law enforcement requirements.

Notice

WWTS notifies all identified data subjects about the purposes for which personal information is collected and used. In certain situations, data is "anonymized" so that the names of the data subjects are not known by data processors within WWTS. In these cases, data subjects do not need to be notified.

Choice

WWTS gives each data subject the opportunity to opt out from allowing WWTS to disclose his/her personal information to a third party or to use it for a purpose incompatible with the purpose for which it was originally collected or authorized. For sensitive data, affirmative choice (opt-in) must be given if the data is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized.

Onward Transfer (to Third Parties)

WWTS may transfer information to a third party acting as an agent for WWTS, such as an outside benefits administrator, by making sure that the third party enters into an agreement with WWTS in which the third party promises to provide the same level of protection as required by the Safe Harbor Privacy Principles.

Security

WWTS takes reasonable precautions to protect personal data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. These precautions include password protections for online information systems and restricted access to personal data processed by HR. All inquiries from outside WWTS, either written or verbal, concerning the identity, employment record, or performance of a current or terminated employee shall be referred, without exception, to HR for handling. If the request is from a government agency, an HR representative and/or the Legal Department will verify the credentials of the agency representative before releasing information about a current or terminated employee.

Data Integrity



WWTS takes reasonable steps to ensure that personal data is accurate, complete, and current. All employees are asked to inform HR and Payroll immediately in the event of changes in personal information.

Access

Upon request, data subjects may access personal information about them and are able to have inaccurate information corrected.

Enforcement

Data subjects may contact the legal department to register complaints, to submit access requests, or to address any other issues arising under the Safe Harbor Privacy Principles.

Martha Morrone
Senior Counsel
Martha.morrone@wwts.com
(978)-848-9103

In addition, the U.S. Federal Trade Commission has authority to hear any claims against WWTS regarding possible unfair or deceptive practices and violations of laws or regulations governing WWTS' privacy practices, including claims alleging WWTS' non-compliance with the Safe Harbor Principles.