

Privacy Policy

Angeion Group

This document was last updated October 27, 2016

Scope: We have developed the following privacy policy to protect individually identifiable information. This policy covers us and applies to all individually identifiable information that we obtain when a client uses our service, including both data processing and online review services. We protect individually identifiable information as follows:

Disclosure: We will not sell, trade, or disclose to third parties any individually (either client or our employee) identifiable information, derived from the use of any of our services, (except as required by subpoena, search warrant or other legal process or in the case of imminent physical harm to the customer or others). When we use other agents, contractors or companies to perform services on its behalf, we will ensure that the company protects the individually identifiable information consistent with this policy

Security: We have implemented technology and security features and strict policy guidelines to safeguard the privacy of identifiable information from unauthorized access or improper use, and we will continue to enhance our security procedures as new technology becomes available.

E-Mail Contents: We will not read or disclose to third parties private e-mail communications that are transmitted using our services except as required to operate the service or as otherwise authorized by law. Improper Conduct: we may use individually identifiable information to investigate and help prevent potentially unlawful activity or activity that threatens the network or otherwise violates the customer agreement for that service. Account Information: we honor requests from clients for changes in account information, such as name and password and will correct any such information that is inaccurate.

Safe Harbor: The United State Department of Commerce and the European Commission have agreed on a set of data protection principles and frequently asked questions (FAQ) (collectively the U.S.-EU Safe Harbor Framework) to enable U.S. companies to satisfy European Union ("EU") law requirements for adequate protection of personal information transferred from the European Economic Association ("EEA") to the United States. The United State Department of Commerce and the Federal Data Protection and Information Commissioner of Switzerland have agreed on a similar set of data protection principles and frequently asked questions (FAQ) (collectively the U.S.-Swiss Safe Harbor Framework) to enable U.S. companies to satisfy Swiss law requirements for adequate protection of personal information transferred from Switzerland to the United States. We comply 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. We have 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 our certification, please visit <http://www.export.gov/safeharbor/>. We adhere to the Safe Harbor Principles outlined below.

Privacy Principles: The privacy principles in this policy are based on the Safe Harbor Principles.

Notice and Choice: We do not collect personal information directly from individuals in the EU or Switzerland. Personal information may exist in electronic discovery information that is provided to us from an EEA organization or Switzerland for processing. To the extent permitted in the Safe Harbor Agreement, we reserve the right to process personal information in the course of providing electronic discovery services to our clients without the knowledge of individuals involved.

Onward Transfers and Disclosures to Agents: We will not knowingly disclose an individual's personal information to third parties, except when one or more of the following conditions is true: * We have the individual's permission to make the disclosure. * The disclosure is required by law or professional standards. * The information is question is publicly available. * The disclosure is reasonably necessary for the establishment or defense of legal claims.

Data Security: We take data security seriously and has put in place appropriate physical, electronic, and procedures to safeguard and secure the information we process.

Data Integrity: We will use personal information only in ways that are compatible with the purposes for which it was collected, which is in the confines of electronic discovery usage.

Access: Upon request, we will grant individuals reasonable access to personal information that it holds about them. In addition, we will take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete.

Enforcement: We utilize the self-assessment approach to assure its compliance with this privacy statement. We periodically verify that the policy is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented, and in conformity with the Safe Harbor Principles. All disputes related to our Safe Harbor policy will be resolved through the dispute resolution procedures of JAMS (www.jamsadr.com).

Changes in Practices: We reserve the right to unilaterally change this policy at any time. We will keep this policy current and post the most current version on our corporate website. If you wish to be informed of any changes that we make please contact us at the address at the end of this document.