

## **Policies and Procedures for Handling Personal Data or Information Subject to EU Safe Harbor Privacy Protection TechLaw Solutions**

The European Union's *Directive on Data Protection* requires that transfers of personal data and information take place only to companies in non-EU countries that provide an "adequate" level of privacy protection. The U.S. Department of Commerce, in conjunction with the EU, defined this "adequacy standard" by establishing the "Safe Harbor" principles.

The Commerce department set out seven Safe Harbor principles to be followed by any U.S. organization receiving personal data from the European Union for the purpose of qualifying for the Safe Harbor and the presumption of "adequacy" it creates. Failure to comply with such self-regulation may be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts, or other law or regulation prohibiting such acts.

The principles, and the policies and procedures implemented by TechLaw Solutions (TechLaw) to meet the requirements of each of these principles, are provided below.

**Principle 1 – Notice.** Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

*TechLaw Solutions Policy:*

1. TechLaw Solutions will verify that any data we receive from the EU subject to Safe Harbor protection was collected by another party (i.e. our client or our client's agent), and that it is not directly from the individual in the EU. Document Processing Center (DPC) policy with regard to data sent to TechLaw by our EU client/agent (and not an individual) is that the EU Client has notice requirement, and that any request for Personal Data information in the possession of the TechLaw Solutions (including making any changes) needs to originate through the EU Client.
2. TechLaw Solutions will ensure this notice requirement is an EU Client responsibility in our agreement with that client.
3. TechLaw Solutions will only use the data we receive for a purpose approved under agreement with our EU Client.

**Principle 2 – Choice.** Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

*TechLaw Solutions Policy:*

1. TechLaw Solutions policy with regard to data sent to us by our EU client/agent (and not an EU individual) is that the EU Client has to give EU individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or

subsequently authorized by the individual. This EU Client responsibility will be included in our agreement with that client.

2. TechLaw Solutions policy with regard to data sent to us by our EU client/agent (and not an EU individual) is that the EU Client has to provide the explicit choice to opt in to allow disclosure of sensitive personal information to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual. This EU Client responsibility will be included in our agreement with that client.
3. TechLaw Solutions policy is that we will only use the data we receive for a purpose approved under agreement with our EU Client.

**Principle 3 – Onward Transfer (Transfers to Third Parties).** To disclose information to a third party, organizations must apply the Notice and Choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

*TechLaw Solutions Policy:*

1. TechLaw Solutions will not disclose EU Privacy Data to a third party until (1) authorized by our EU Client to do so, and (2) we have ensured that the party the information is disclosed to is Safe Harbor certified, or situated in the EU, or bound by a written agreement with TechLaw regarding data protection to at least the same level of privacy protection as is required by the relevant principles.
2. An exception would be a legal duty to provide the information.

**Principle 4 – Access.** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. TechLaw will make changes to the data if found to be inaccurate, as directed by the EU Client.

*TechLaw Solutions Policy:*

TechLaw Solutions will allow an individual access to their data if the EU Client approves, and if the burden is not excessive and disproportionate to the individual's privacy, or where the rights of another person might be violated.

**Principle 5 – Security.** Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

*TechLaw Solutions Policy:*

TechLaw Solutions will properly track and secure EU Privacy Data while it is in its possession and will limit its access to TechLaw Solutions employees on a need to know basis.

**Principle 6 – Data integrity.** Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

*TechLaw Solutions Policy:*

TechLaw Solutions will process the data only for the purpose approved under agreement with our EU Client. TechLaw Solutions will properly track and secure EU Privacy Data while it is in our possession and will limit its access to TechLaw Solutions employees on a need to know basis.

**Principle 7 – Enforcement.** In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

*TechLaw Solutions Policy:*

1. TechLaw Solutions will periodically audit, at the rate of at least once per year, our procedures with regards to any processing of Safe Harbor protected data. This audit will be conducted by TechLaw Solutions personnel not part of the Data Processing Center (DPC) staff. Any problems discovered will be corrected and procedures modified as appropriate.
2. TechLaw Solutions will also respond to any individual's complaint or dispute regarding its handling of Safe Harbor protected data.
3. TechLaw Solutions will implement its Safe Harbor policies through the use of the procedures provided in the following three documents:

*Safe Harbor [New Matter] Process Flow.* This document will be used by TechLaw Solutions to outline the steps that are to be taken and followed any time we receive a new matter with Safe Harbor protected data.

*[New Matter] – Safe Harbor Data Monitoring Form.* This form will be used by TechLaw Solutions to track any Safe Harbor protected media or documents received, including what was received, where it was stored, when it was produced, whether any request was received to review the data, whether any changes were made to the original data, when the data was returned, and when the Safe Harbor protection process was audited.

*[New Matter] Security for Data Subject to EU Safe Harbor Privacy Protection.* This document will be used by TechLaw Solutions to outline the steps that are to be taken to protect Safe Harbor personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.