Last updated April 17, 2020

AgilePoint, INC a Delaware company (AgilePoint) complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data (as defined below) from European Union member countries and Switzerland. AgilePoint has certified that it adheres to the Privacy Shield Principles of Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement, and Liability. If there is any conflict between the policies in AgilePoint's Privacy Shield Policy (“Privacy Shield Policy”) and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/.

Definitions

“Data Owner” means the individual to whom any given Personal Data covered by this Privacy Shield Policy refers.

“Personal Data” means any information relating to an individual residing in the European Union and Switzerland that can be used to identify that individual either on its own or in combination with other readily available data.

“Sensitive Personal Data” means Personal Data regarding an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, physical or mental health, or sexual life.

Scope and Responsibility

This Privacy Shield Policy applies to Personal Data transferred from European Union member countries and Switzerland to AgilePoint's operations in the U.S. in reliance on the respective Privacy Shield framework and does not apply to Personal Data transferred under Standard Contractual Clauses or any approved derogation from the EU Directive.

Some types of Personal Data may be subject to other privacy-related requirements and policies. For example:

Personal Data held by an AgilePoint customer using AgilePoint NX is also subject to any specific agreement with, or notice to, the customer, as well as additional applicable laws and professional standards.

Employee Personal Information is subject to internal human resource policies including the Employee Data Privacy Notice.

All AgilePoint employees that have access in the U.S. to Personal Data covered by this Privacy Shield Policy are responsible for conducting themselves in accordance with this Privacy Shield Policy. Adherence by AgilePoint to this Privacy Shield Policy may be limited to the extent required to meet legal, regulatory, governmental, or national security obligations, but Personal Data covered by this Privacy Shield Policy shall not be collected, used, or disclosed in a manner contrary to this policy without the prior written permission of AgilePoint’s CSO.
AgilePoint employees responsible for engaging third parties to which Personal Data covered by this Privacy Shield Policy will be transferred are responsible for obtaining appropriate assurances that such third parties have an obligation to conduct themselves in accordance with the applicable provisions of this Privacy Shield Principles, including any applicable contractual assurances required by Privacy Shield.

Privacy Shield Principles

AgilePoint commits to subject to the Privacy Shields’ Principles all Personal Data received by AgilePoint in the U.S. from European Union member countries and Switzerland in reliance on the respective Privacy Shield framework.

1. Notice

AgilePoint notifies Data Owners covered by this Choice Privacy Shield Policy about its data practices regarding Personal Data received by AgilePoint in the U.S., from European Union member countries and from Switzerland in reliance on the respective Privacy Shield framework, including:

(i) the types of Personal Data it collects about them, the purposes for which it collects and uses such Personal Data,
(ii) the types of third parties to which it discloses such Personal Data and the purposes for which it does so,
(iii) the rights of Data Owners to access their Personal Data,
(iv) the choices and means that AgilePoint offers for limiting its use and disclosure of such Personal Data,
(v) how AgilePoint’s obligations under the Privacy Shield are enforced,
(vi) and how Data Owners can contact AgilePoint with any inquiries, updates or complaints.

2. Choice

If Personal Data covered by this Privacy Shield Policy is to be used for a new purpose that is materially different from that for which the Personal Data was originally collected or subsequently authorized, or is to be disclosed to a third party, AgilePoint will provide Data Owners with an opportunity to choose whether to have their Personal Data so used or disclosed. Requests to opt out of such uses or disclosures of Personal Data should be sent to ap-privacy@agilepoint.com.

If Sensitive Personal Data covered by this Privacy Shield Policy are to be used for a new purpose that is different from that for which the Personal Data was originally collected or subsequently authorized, or the Personal Data is to be disclosed to a third party, AgilePoint will obtain the Data Owner’s explicit consent prior to such use or disclosure.

3. Accountability for Onward Transfer

In the event AgilePoint transfers Personal Data covered by this Privacy Shield Policy to a third party acting as a controller, AgilePoint will do so consistent with any notice provided to Data Owners and any consent they have given, and only if the third party has given us contractual assurances that it will:
(i) process the Personal Data for limited and specified purposes consistent with any consent provided by the Data Owners,
(ii) provide at least the same level of protection as is required by the Privacy Shield Principles and notify AgilePoint if it makes a determination that they cannot do so,
(iii) cease processing of the Personal Data or take other reasonable and appropriate steps to remediate if they make such a determination.

If AgilePoint has knowledge that a third party acting as a controller is processing Personal Data covered by this Privacy Shield Policy in a way that is contrary to the Privacy Shield Principles, AgilePoint will take reasonable steps to prevent or stop such processing.

Employment-related operational needs with respect to personal data transferred under the Privacy Shield for activities such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, provided that the Privacy Shield organization has complied with the Notice and Choice Principles.

With respect to AgilePoint Partners, we will transfer only the Personal Data covered by this Privacy Shield Policy needed for a Partner to deliver to its customers the AgilePoint product or service. Furthermore, AgilePoint will:

(i) permit the Partner to process such Personal Data only for limited and specified purposes,
(ii) require the Partner to provide at least the same level of privacy protection as is required by the Privacy Shield Principles,
(iii) take reasonable and appropriate steps to ensure that the Partner effectively processes the Personal Data transferred in a manner consistent with AgilePoint’s obligations under the Privacy Shield Principles,
(iv) require the Partner to notify AgilePoint if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles.

Upon receiving notice from a Partner that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles, AgilePoint will take reasonable and appropriate steps to stop and remediate unauthorized processing.

AgilePoint remains liable under the Privacy Shield Principles if a Partner processes Personal Data covered by this Privacy Shield Policy in a manner inconsistent with the Principles, except where AgilePoint is not responsible for the event giving rise to the damage.

4. Security

AgilePoint takes reasonable and appropriate measures to protect Personal Data covered by this Privacy Shield Policy from loss, misuse, unauthorized access, disclosure, alteration, and destruction. This is done while taking into account the risks involved in the processing and the nature of the Personal Data.
5. Data Integrity and Purpose Limitation

AgilePoint limits the collection of Personal Data covered by this Privacy Shield Policy to information that is relevant for the purposes of deploying AgilePoint product and services. AgilePoint does not process such Personal Data in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the Data Owner.

AgilePoint takes reasonable steps to ensure that such Personal Data is reliable for its intended use, accurate, complete, and current. AgilePoint takes reasonable and appropriate measures to comply with the requirement under the Privacy Shield to retain Personal Data in identifiable form only for as long as it serves a purpose of processing, which includes AgilePoint’s obligations to comply with professional standards, AgilePoint’s business purposes and unless a longer retention period is permitted by law, and the Privacy Shield Principles are adhered to for as long as AgilePoint retains such Personal Data.

6. Access

Data Owners whose Personal Data is covered by this Privacy Shield Policy have the right to access such Personal Data and to correct, amend, or delete such Personal Data if it is inaccurate or has been processed in violation of the Privacy Shield Principles (except when the burden or expense of providing access, correction, amendment, or deletion would be disproportionate to the risks to the Data Owner’s privacy, or where the rights of persons other than the Data Owner would be violated).

Requests for access, correction, amendment, or deletion should be sent to ap-privacy@agilepoint.com

7. Recourse, Enforcement, and Liability

AgilePoint’s participation in the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework is subject to investigation and enforcement by the Federal Trade Commission.

In compliance with the Privacy Shield Principles, (your organization name) commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact AgilePoint at ap-privacy@agilepoint.com

AgilePoint has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning data transferred from the EU. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please visit https://edpb.europa.eu/about-edpb/board/members_en for more information or to file a complaint.

AgilePoint has further committed to cooperate with the Swiss Federal Data Protection and Information Commissioner (FDPIC) and comply with the advice given by such authorities with regard to human resources data transferred from Switzerland in the context of the employment relationship.
In certain conditions, the individual has the right to invoke binding arbitration. Data Owners with inquiries or complaints regarding this Privacy Shield Policy should first contact AgilePoint at ap-privacy@agilepoint.com.

AgilePoint is required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

AgilePoint agrees to periodically review and verify its compliance with the Privacy Shield Principles, and to remedy any issues arising out of failure to comply with the Privacy Shield Principles. AgilePoint acknowledges that its failure to provide an annual self-certification to the U.S. Department of Commerce will remove it from the Department’s list of Privacy Shield participants.

Changes to this Privacy Shield Policy

This Privacy Shield Policy may be amended from time to time consistent with the requirements of the Privacy Shield. Appropriate notice regarding such amendments will be given.