EU-U.S. Privacy Shield Policy

This Privacy Shield Policy (the "**Policy**") details how EisnerAmper (as defined below) in the United States ("**U.S.**") collects, uses, and discloses personal data that we receive in the U.S. from the European Union ("**EU**"). This Notice supplements our Privacy Policy located at: https://www.eisneramper.com/privacy_policy/ and is incorporated therein by this reference.

For the purposes of this Policy, the following definitions shall apply:

"**EisnerAmper**" means EisnerAmper LLP, and EisnerAmper Global Compliance & Regulatory Solutions LLC.

"**data subject**" means an identified or identifiable natural person

"**identifiable natural person**" means a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Personal data**" means any information relating to a data subject.

"**Processing**" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

"**Privacy Shield Principles**" means those principles set forth at https://www.privacyshield.gov/article?id=Requirements-of-Participation.

Participation in Privacy Shield

EisnerAmper recognizes that the EU has established protections regarding the handling of personal data, including requirements to provide adequate protection for personal data transferred outside of the EU. To provide sufficient privacy controls for personal data pertaining to EisnerAmper clients, vendors, and business partners in the EU which is received by the firm in the US, EisnerAmper has elected to self-certify to the EU-U.S. Privacy Shield Framework administered by the U.S. Department of Commerce ("**Privacy Shield**").

To learn more about the Privacy Shield Framework, and to view EisnerAmper's certification, please visit https://www.privacyshield.gov.

Enforcement Jurisdiction

EisnerAmper is subject to the investigatory and enforcement powers of the Federal Trade Commission.

Types of Personal Data Collected

EisnerAmper collects and processes the types of personal data as set forth below:

- Personal data regarding current, former and prospective partners, principals and employees. Collected partner, principal, and employee data includes names, addresses, phone numbers, email addresses, date of birth, citizenship status, next of kin, tax and personal identification numbers, marital status, and bank account numbers.
- Personal data regarding current, former and prospective clients, their clients, and their respective personnel and other parties. Collected data in this category includes names, addresses, phone numbers, email addresses, tax and personal identification numbers, and bank account numbers.
- Personal data regarding our third party service providers and their personnel. Collected third party service provider data includes names, addresses, phone numbers, and email addresses of the service provider's personnel.
- Additionally, EisnerAmper may, from time to time, collect personal information from the general public in order to answer inquiries or provide information requested, including through the use of our Website, www.EisnerAmper.com, in which case, such collection is also subject to the terms of our Privacy Policy. Collected general public data includes names, addresses, phone numbers, and email addresses.

Purposes for Collection and Processing of Personal Data

EisnerAmper is a limited liability partnership, provides comprehensive audit, accounting, advisory, consulting, and tax services. Personal data for current, former and prospective partners, principals and employees is used for the purposes of operating and managing EisnerAmper, performing internal human resource administration (e.g., payroll management, benefits administration), and maintaining contact with individuals (e.g., to reach out to notify employees of emergencies).

Personal data for current, former, and prospective clients, their clients and personnel, is used for the purposes of delivering EisnerAmper services (audit, accounting, advisory, consulting, and tax services), maintaining ongoing relationships (e.g., sending invoices, and notifying clients and prospective clients of changes to EisnerAmper services), and performing business development activities (e.g., sending notices pertaining to changes in laws or professional standards, and sending thought leadership pieces in fields of interest to the recipients).

Personal data for third party service providers is used for the purposes of obtaining services (e.g., such as obtaining data hosting services, obtaining access to and use of software as a service offerings and tax preparation software, etc.), and managing and administering EisnerAmper business relationships with such third parties (e.g., communicating with service provider personnel about upcoming changes to services or EisnerAmper needs, requesting copies of and paying invoices, etc.).

Personal data from the general public is used for the completion of performance surveys and relaying information on professional services provided by EisnerAmper, and to respond to and comply with opt-out and other requests from data subjects (as set forth below).

Under EisnerAmper's security program, personal data is processed for EisnerAmper business purposes only.

How we Collect and Process Personal Data

EisnerAmper collects personal data (i) directly from its clients when such clients or their employees or agents provide it to us for the purpose of performing our services or managing the relationship, or as we may learn from such persons during the business relationship of the parties; (ii) when it is submitted to us through our Website, or when an individual sends us correspondence through e-mail or postal mail; (iii) when an employee or partner is initially engaged and throughout the employment/partnership relationship; obligations; and (iv) when initiating a vendor/service provider relationship, at which point contact information of various persons is provided to us in order to maintain the relationship.

All such personal data is collected, processed, and stored by EisnerAmper (or through processors/sub-processors) as electronic or physical files.

Processors/Sub-Processors

EisnerAmper utilizes processors/sub-processors as part of its business. The list of such processors and sub-processors is available upon reasonable request.

All personal data as described in "Types of Personal Data Collected" above are shared with service providers, to enable EisnerAmper to provide its services and process the data for the purposes set forth above in Section titled "Purposes for the Collection and Processing of Personal Data". This means that personal data may be shared with service providers for the purpose of data hosting, or in the course of EisnerAmper preparing tax returns, sharing documents or information with our clients, providing financial advisory services, conducting audits and providing consulting services.

Clients have the right to object to our use of certain processors or sub-processors under specific circumstances. If you are our client and have any concern with any processors or sub-processors we use, please let us know, and we will work with you to try to resolve your concerns (which may include removing your data from a particular processor's or sub-processor's possession or access).

Commitment to be Subject to Privacy Shield Principles

EisnerAmper has committed to adhere to the Privacy Shield Principles, including using the personal data collected only for the purposes it was collected. EisnerAmper may occasionally also send certain individuals communications it deems of value to such persons, but which the individual can opt out of.

Notice and Choice

Notice to individuals regarding the personal data collected from them and how that information is used may be provided through this Policy, other website notices, or other direct forms of communication with appropriate parties, such as contracts or agreements.

As a data subject whose personal data we have collected, you have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

(a) If you want us to establish the data's accuracy.

(b) Where our use of the data is unlawful but you do not want us to erase it.

(c) Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.

(d) You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights).

However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Accountability for Onward Transfer

Except as instructed by the controller of personal data or the individual data subject, EisnerAmper will not transfer any personal data of EU persons to a third party without first ensuring that the third party adheres to the Privacy Shield Principles, unless such entity adheres to security controls and procedures which EisnerAmper considers to be adequate.

We, EisnerAmper, remain responsible for the acts and omissions of our sub-processors in the event of an onward transfer of your personal data to such sub-processors.

Security

EisnerAmper maintains security protocols consistent with guidelines set by the International Organization for Standardization System and Organization Controls (ISO SOC) to protect personal data from loss, unauthorized access, disclosure, alteration and destruction.

Access and Correction

Upon request, EisnerAmper will grant individuals who are its clients reasonable access to the personal data the firm retains about them. EisnerAmper will also take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or has been processed in violation of the firm's contracted services.

Verification

EisnerAmper assures compliance with this Policy by utilizing the self-assessment approach as specified by the U.S. Department of Commerce. The assessment will be conducted on an annual basis to ensure that EisnerAmper's security and privacy practices as set forth herein are being followed in adherence with this Policy. EisnerAmper personnel found to be in violation of this Policy may be subject to disciplinary measures, up to and including termination of employment.

Recourse, Enforcement and Liability

Any complaints or concerns regarding the use or disclosure of personal data transferred from the EU to the firm in the U.S. should, in the first instance, be directed to the EisnerAmper Information Security and Privacy Director, or the VeraSafe Alternative Dispute Resolution provider. Their contact information is set forth at the end of this Policy.

You may have the option to select binding arbitration under the Privacy Shield Panel (as described in https://www.privacyshield.gov/article?id=B-Available-Remedies) for the resolution of your complaint under certain circumstances. For further information, please see the Privacy Shield website.

Law Enforcement and National Security

Please be advised that EisnerAmper may at times be required to disclose your personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Limitation on Scope of Principles

Adherence by EisnerAmper to the Privacy Shield Principles may be limited (a) to the extent the firm is required to respond to a legal obligation; and (b) to the extent permitted by an applicable law or regulation.

Changes to this Policy

This Policy may be amended from time to time, consistent with the requirements of applicable laws and regulations. Revisions will be in effect upon the date of publication.

Contact Information

Questions or comments related to this Policy, data processing or data collection should be submitted to the VeraSafe Alternative Resolution Service support line or the EisnerAmper Information Security and Privacy Director:

VeraSafe Alternative Resolution Service Hotline

1-888-376-1079, support@VeraSafe.com, www.VeraSafe.com

Todd Gordon, EisnerAmper Director of Information Security and Privacy

212-891-8020, todd.gordon@eisneramper.com