

YourEncore's Privacy Shield Notice

YourEncore is strongly committed to protecting the privacy of our clients. This notice outlines our general policy and practices for implementing the Privacy Shield Principles, including the type of information to which this notice applies, how we use personal information, and the choices individuals have regarding our use of, and their ability to access and correct, that personal information. If there is any conflict between the policies in this notice and the Privacy Shield Principles, then the Privacy Shield Principles will govern.

E.U.-U.S. Privacy Shield

YourEncore recognizes that the European Union ("E.U.") has established strict protections regarding the handling of E.U. personal information, including requirements to provide adequate protection for E.U. personal information transferred outside of the E.U. YourEncore complies with the E.U.-U.S. Privacy Shield framework as agreed to between the U.S. Department of Commerce and the European Commission regarding the collection, use, and retention of personal information from E.U. member countries. YourEncore 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. To learn more about the Privacy Shield program, and to view YourEncore's certification, please visit the Privacy Shield website at www.privacyshield.gov. As a Privacy Shield participant, we have agreed to abide by the investigatory and enforcement powers of the U.S. Federal Trade Commission or any other U.S. authorized statutory body.

This notice applies to all personal information we obtain through our provision of services. For purposes of this notice, "personal information" means data that:

- is transferred from the E.U. to the U.S.;
- is recorded in any form; and
- is about, or pertains to, a specific individual who is identified in, or is identifiable from, the data.

"Sensitive information" is a subcategory of personal information. Sensitive information is defined as personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or the sex life of the individual. Sensitive information also includes personal information received from a third party where the third party treats and identifies it as sensitive.

Privacy Shield Principles Regarding Personal Information

Notice

We notify individuals about the personal information we collect from them, how we use it, and how to contact us with privacy concerns. We obtain personal information only as permitted by the Privacy Shield Principles or with the consent of the individual affected. Consent for personal information to be collected, used, and/or disclosed in certain ways may be required in order for an individual to obtain or use our services.

YourEncore provides advisory services for consumer products, life sciences, and food sciences in Europe, Asia, Australia, and the Americas. The types of personal information that we may collect in order to provide services to clients include, but are not limited to: (1) first and last names of clients' points of contact; (2) mailing addresses; (3) email addresses; (4) telephone numbers; and (5) billing information. We collect personal information from our clients for various purposes, which include, but are not limited to: (1) providing our services to our clients; (2) communicating with our clients regarding the provision of services to them; (3) assessing the quality and effectiveness of the services we provide to our clients; and (4) marketing our products and services.

Choice

To the extent permitted under the Privacy Shield, we reserve the right to process personal information in the course of providing professional services to our clients in a manner consistent with the purposes for which the information is collected, without the knowledge of individuals involved.

When required by the Privacy Shield, we offer individuals the opportunity to opt out of disclosures of personal information to a third party or the use of personal information for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individual.

We will comply with the Privacy Shield Principles with respect to disclosures of sensitive information, including, when applicable, obtaining the explicit consent (i.e., opt in consent) of the individual prior to disclosing sensitive information to a third party or using sensitive information for purposes other than those for which it was originally collected or subsequently authorized by the individual.

Accountability for Onward Transfers

We are potentially liable in cases of onward transfers of personal information to third parties, such as when third parties that act as agents on our behalf process personal information in a manner inconsistent with the Privacy Shield Principles. We will ensure that any third party to

which we disclose personal information provides the same level of privacy protection as is required by the Privacy Shield principles and agrees in writing to provide an adequate level of privacy protection.

We may transfer personal information to third-party agents, or service providers, who perform functions on our behalf, such as vendors for customer relationship management, professional services planning, and project accounting. We enter into written agreements with those third-party agents and service providers requiring them to provide the same level of protection the Privacy Shield requires and limiting their use of the data to the specified services provided on our behalf.

Under some circumstances, we may be required to disclose personal information when necessary to respond to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Data Security and Integrity

We employ administrative, technical, and physical safeguards, including education and training of our personnel, designed to provide the personal information in our possession with reasonable protection loss, misuse, unauthorized access, disclosure, alteration, or destruction. Personal information collected or displayed through a website is protected in transit by industry standard encryption processes. However, we cannot guarantee the security of personal information accessible on or transmitted via the Internet.

We process personal information in ways compatible with the purpose for which the personal information was collected, or as otherwise authorized by the individual. To the extent necessary for such purposes, we take reasonable steps to make sure that personal information is accurate, complete, current, and otherwise reliable with regard to its intended use.

Access

You have the right to obtain our confirmation of whether we maintain personal information relating to him or her. Upon request, we will provide you access to your personal information within a reasonable time period. If an individual becomes aware that personal information we maintain about that individual is inaccurate, or if an individual would like to update, delete, review his or her personal information, the individual may contact us using the contact information below. In addition, we may limit or deny access to personal information where providing such access would be unreasonably burdensome or expensive in the circumstances, or as otherwise permitted by the Privacy Shield. If we determine that your access should be restricted in a particular instance, we will provide you with an explanation of our determination

and respond to any inquiries you may have. In some circumstances, we may charge a reasonable fee, where warranted, for access to personal information.

Recourse, Enforcement, and Liability

We commit to internally resolving your complaints related to our privacy practices or our collection, or use, or disclosure of personal information. We will respond to your complaint within forty-five (45) days of receipt. You may file a privacy complaint by contacting us at our contacting information below.

We also agree to participate in independent dispute resolution with the E.U. data protection authorities (DPAs). We will cooperate with the DPAs in the investigation and resolution of complaints brought under the Privacy Shield and we agree to comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Privacy Shield Principles.

Please note that if an individual's complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

Amendment

We may amend this notice from time to time by posting a revised notice on this website, or a similar website that replaces this website. If we amend the notice, the new notice will apply to personal information previously collected only insofar as the rights of the individual affected are not reduced. As long as we profess to adhere to the Privacy Shield Principles, we will not amend this notice in a manner inconsistent with the Privacy Shield Principles.

Contact Information

To request access to personal information, inquire about this privacy policy, or file a privacy complaint, an individual may contact us at:

Attn: Tim Tichenor
Chief Financial Officer
YourEncore, Inc.
20 North Meridian Street, Suite 800
Indianapolis, Indiana 46204