EU-U.S. Privacy Shield

The United States Department of Commerce has worked with the European Commission to develop the EU-U.S. Privacy Shield to allow U.S. companies to meet the EU law requirements that Personal Data transferred from the EU to the United States be adequately protected. Consistent with its pledge to protect personal privacy, we adhere to the Privacy Shield Principles. If there is any conflict between the policies in this privacy 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/list.

Scope

This Personal Data Protection Policy (the "Policy") applies to all Personal Data received by us in the United States from the EU and/or other applicable countries, recorded in any form (including electronic, paper or verbal).

Definitions

The following definitions shall apply throughout this Policy:

- "Agent" means any third party that uses Personal Data provided to us to perform tasks on behalf of and under the instructions of us.
- "Personal Data" means Information or a set of information that identifies or could be used by or on behalf of us to identify an individual. Personal Data does not include information that is encoded, anonymous, aggregated or publicly available information that has not been combined with non-public Personal Data.
- "Sensitive Personal Data" means Personal Data that reveals racial, ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership or information that specifies the health or sex life of the individual. In addition, we will treat any information as Sensitive Personal Data which received from a third party where that third party treats and identifies the information as sensitive.

Privacy Principles

The privacy principles in this Policy are based on the Data Protection Directive and Privacy Shield Principles.

1. Notice
When we collect Personal Data directly from individuals in the EU and/or other applicable countries, we will inform them about the purposes for which we collect and use their Personal Data, the types of third parties (other than Agents), if any, to which we disclose that information, and the choices and means, if any, that we offer individuals for limiting the use and disclosure of their Personal Data. Notice will be provided in clear and conspicuous language when individuals are first asked to provide Personal Data to us, or as soon as practicable thereafter, and in any event before we use the information for a purpose other than that for which it was originally collected. If we receive Personal Data from our affiliates or other entities in the EU and other countries with which we do business, we will use such information in accordance with the notices such entities provided and the choices made by the individuals to whom such Personal Data relates.

2. Choice
We will offer individuals the opportunity to choose (opt-out) whether their Personal Data is (a) to be disclosed to a third party (other than an Agent), or (b) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

For Sensitive Personal Data, we will give individuals the opportunity to affirmatively and explicitly (opt-in) consent to (a) the disclosure of the information to a third party, or (b) the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. We will provide individuals with reasonable methods to exercise their choices.

We may disclose personal information to third parties in the following instances:

Website Consultants and Service Providers. We may disclose personal information to third party consultants and service providers (such as providers of hosting services, support, maintenance and remedial and repair services) to the extent that they require access to our databases, or the

information contained in our databases, to service us and our customers under the conditions set out in the Principles.

Enforcement of Rights / Security. We reserve the right to release personal information (i) when we are under legal compulsion to do so (e.g. we have received a subpoena) or we otherwise believe that the law requires us to do so, (ii) when we believe it is necessary to protect and/or enforce the rights, property interests, or safety of us, our customers or others, or (iii) as we deem necessary to resolve disputes, troubleshoot problems, prevent fraud and/or enforce the Principles.

Reorganization or Sale. In the event that our company is merged with or becomes part of another organization, or in the event that our company is sold or it sells all or substantially all of its assets or is otherwise reorganized, the information you provide may be one of the transferred assets to the acquiring or reorganized entity.

As Otherwise Allowed by Law. We may transfer personal information to third parties where we are expressly authorized by applicable law and the Principles to do so. We also may be required to disclose an individual's personal information in response to a lawful request by public authorities, including meeting national security or law enforcement requirements.

3. Accountability For Onward Transfers
We will obtain assurances from our Agents that they will safeguard Personal Data consistently with this policy. If we have knowledge that an Agent is using or disclosing Personal Data in a manner contrary to this policy, we will take reasonable steps to prevent or stop the use or disclosure. In cases of Onward Transfer InMoment, Inc. remains liable.

4. Security
We will take reasonable precautions to protect Personal Data in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction.

5. Data Integrity & Purpose Limitation
We will use Personal Data only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. We will take reasonable steps to ensure that Personal Data is relevant to its intended use, accurate, complete, and current.

6. Access
Upon request, we will grant individuals reasonable access to Personal Data that we hold about them, and we will take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete.

7. Recourse, Enforcement And Liability
We will conduct compliance audits of our relevant privacy practices to verify adherence to this Policy. Any employee that we determine is in violation of this Policy will be subject to disciplinary action up to and including termination of employment.

Dispute Resolution and Enforcement

Any questions or concerns regarding the use or disclosure of Personal Data should be directed to us at the address given below. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data in accordance with the principles contained in this Policy within 45 days of receiving a complaint. For complaints that cannot be resolved between us and the complainant, we have agreed to participate in the dispute resolution procedures pursuant to the Privacy Shield Principles.

If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please contact our US-based third-party dispute resolution provider (free of charge) at feedback-form.truste.com/watchdog/request.

We are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). Should an individual be unable to resolve a complaint with us, they may contact the FTC at the following address:

Federal Trade Commission
Attn: Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
www.ftc.gov.

EU Persons (EU Data Subjects) may make complaints to their home data protection authority and can invoke binding arbitration for some residual claims not resolved by other redress mechanisms. These conditions are more fully described on the Privacy Shield website at: https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint.

3rd Party Dispute Resolution

If you have any other unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Contact Information

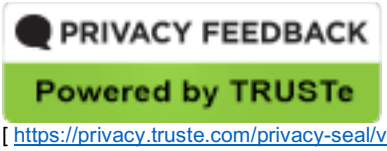
Questions or comments regarding this Policy, as well as any Privacy Shield related complaints, should be submitted to us by mail or e-mail as follows:

Company Name and Contact: General Counsel Attn: Legal Inmoment.com
Address: 10355 South Jordan Gateway, Suite 600, South Jordan, Utah, USA 84095
Email: legal@inmoment.com

For any Privacy Shield related complaints that are not resolved within 45 days, you may file a complaint with our independent dispute resolution provider at the following website: https://feedback-form.truste.com/watchdog/request.

Changes to Personal Data Protection Policy

This Policy may be amended from time to time, consistent with the requirements of the Data Protection Directive and/or Privacy Shield Principles. We will provide appropriate public notice about such amendments.



[https://privacy.truste.com/privacy-seal/validation?rid=7255a80e-06a3-447a-8ff3-57c5d8316680]