LLamasoft Privacy Shield Statement

Privacy Shield Privacy Statement under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield

Privacy Shield is a program administered by the United States Department of Commerce (the “Department”).

We comply with both 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 information transferred from the European Union, the United Kingdom and Switzerland, respectively, to the United States. We have certified to the Department of Commerce that we adhere to the Privacy Shield Principles that are a part of the Privacy Shield program (the “Principles”). To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

This Privacy Shield Privacy Statement describes the Privacy Principles and tells you how we comply with those Principles.

When we say “we” or “our” or words like those, or “LLamasoft” we mean LLamasoft, Inc., a Delaware, USA corporation. LLamasoft, Inc., together with any subsidiaries and affiliates, are the “LLamasoft Enterprise” and each of them is a “LLamasoft Enterprise Company.”

Scope

This Privacy Statement covers transfers of personal data under both the EU-U.S. Privacy Shield Framework (a program agreed upon by the European Commission and the United States government) and the Swiss-U.S. Privacy Shield Framework (a very similar program agreed upon by the Swiss and United States governments). This Privacy Statement speaks of these frameworks as the “Privacy Shield” or the “Privacy Shield program.”

The “European Union,” or “EU,” consists of Austria, Belgium, Bulgaria, Croatia, the Republic of Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden. The “European Economic Area” or “EEA” consists of all of the EU member states, plus Iceland, Liechtenstein and Norway.

This Privacy Shield Privacy Statement covers personal data about data subjects who are citizens of any EEA member state, or of Switzerland, where the personal data is transferred to, and/or processed in, the United States

If a data subject gives his or her consent to the export of his/her personal data to the United States, and/or processing of his or her personal data in the United States, that consent governs such export and processing and this Privacy Shield Privacy Statement doesn’t apply to any export or processing within the scope of that consent. To the extent that the data subject’s consent does not apply, this Privacy Shield Privacy Statement will apply.

Some Important Concepts

The Privacy Shield program and its Privacy Principles use certain terms that are defined by European law. Here are some of those terms.

“Personal data” for the purposes of the EU-U.S. Privacy Shield means any information relating to an identified or identifiable natural person. For the purposes of the Swiss-U.S. Privacy Shield, the term means personal data that is within the scope of the Swiss Federal Act on Data Protection (“FADP”).

“Sensitive information” under the EU-U.S. Privacy Shield means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or health or sex life. “Sensitive information” under the Swiss-U.S. Privacy Shield program means personal information specifying medical or health conditions, personal sexuality, racial or ethnic origin, political opinions, religious, ideological or trade union-related views or activities, or information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.

A “natural person” is a human being. The law sometimes treats corporations and other business entities as “persons,” so using the term “natural person” makes it clear that we’re talking about a human being.

A “data subject” is the identified or identifiable natural person to which the personal data relates.

An “identifiable natural person” is one 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.

“Processing” of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

A “controller” of personal data is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

A “processor” of personal data is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The Way We Refer to the Personal Data that We Collect

We collect, maintain, use, and share “Business Personal Data” and “Human Resources Personal Data.” Here’s what we mean by those terms.

> “Business Personal Data” is personal data that enables identification of, authentication of, coordination of, and/or communication to, from, between, and/or among people who work for or with us, and/or for whom we provide goods or services. These people include, but aren’t limed to, employees, agents, contractors, customers, suppliers, users of our goods and services and others with or through whom we do business or might do business, or for whose benefit we do business. Business Personal Data includes, but is not limited to, contact information, identification information, information about whereabouts, information about travel plans, information about goods and/or services to be provided by (or to) us, applications used, manner and extent of the use of applications, and directory information such as name, mobile and/or land telephone number, fax number, e-mail address, physical address, user ID, IP address, picture, language(s) spoken, title, organizational role, and

systems or processes that such persons are authorized to utilize.

"Human Resource Personal Data" is human resources and benefit information used by one or more LLamasoft Enterprise Companies to evaluate, employ, retain, administer the employment and/or or contractor relationship with, and/or receive or provide the services of, employees and/or direct or indirect contractors who are being considered to do, who do, or have done work for, or for the benefit of, one or more LLamasoft Enterprise Companies.

Other Important Concepts

Where we say that we "anonymize" personal data, that means that we combine it with other information, redact it, or otherwise make it so that it no longer reasonably identifies the data subject.

How We Comply with the Privacy Shield Privacy Principles

We think that the best way to tell you about how we comply with the Principles is to show you the Principles and tell you side-by-side how we comply with them. That way, you get to learn about the Principles and see how our practices line up at the same time.

What the Principles Require.	What we do.
1. NOTICE An organization must inform individuals about:	
Its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List.	We participate in the Privacy Shield and this Privacy Shield Privacy Statement tells you that we participate and how we do it. You can see the Privacy Shield List, and find out more about the Privacy Shield program, at https://www.privacyshield.gov/list.
The types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles.	We collect Business Personal Data and Human Resources Personal data, defined above. Each of the LLamasoft Enterprise Companies collects such data.
Its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield.	We commit to subject to the Principles all of the personal data received from the European Union, the United Kingdom and Switzerland, respectively, in reliance on the Privacy Shield.
The U.S. subsidiaries of the organization also adhering to the Privacy Shield Principles.	Our U.S. subsidiary: Opex Analytics LLC also adheres to the Privacy Shield Principles in the same manner.
The purposes for which it collects and uses personal information about them.	We collect personal data for the following reasons. (a) So that data subjects can be contacted, and/or can contact each other, in order to do business. (b) So that we can provide goods or services to data subjects and/or their organizations and/or receive goods or services from data subjects and/or their organizations. (c) So that we can monitor the use of our goods and services for the purposes of maintenance, improvement, and license compliance. (c) So that we can give to employees, agents, and/or contractors access to the systems and databases that they need to perform their work. (d) So that we can effectively manage human resources, provide opportunities for individuals, and generally make

What the Principles Require.	What we do.
	advice and analyses available regarding employer-employee and contractor relationships between us and prospective, current, and past employees and/or contractors.
How to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints.	You can contact us using the information below in the section called "**How to Contact Us**."
The type or identity of third parties to which it discloses personal information, and the purposes for which it does so.	(a) Anonymized information. If we anonymize personal data, we may share that personal data with anyone for any purpose. (b) Persons with whom we do business. We may provide personal data to others involved in the provision or receipt of goods and/or services so that we can cooperate in providing or receiving goods and/or services. (c) Outsourcing providers. We may provide personal data to outsourcing providers who perform functions in support of our conduct of business. This might include data processing, storage, system administration, and similar functions. (d) Successors. If we sell or otherwise transfer all or a part of our business, or are investigating the possibility of doing so, we may transfer to, or share with, the actual or potential buyer or other transferee, the personal data associated with the actually or potentially sold or transferred business. (e) To comply with legal requirements. We may share your information if required by law enforcement, government agencies, courts, or others where we believe that our cooperation with information requests is required by law. We provide personal information to others so that we can accomplish the purposes stated above.
The right of individuals to access their personal data.	You have the right to know what personal data we possess about you. You can access that personal data by contacting us using the information below in the section called "**How to Contact U**s."
The choices and means the organization offers individuals for limiting the use and disclosure of their personal data.	You have choices about what personal data we retain and how we use it. See the answers in Principle 2: Choice.
The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by [Data Protection Authorities, sometimes called] DPAs or, in the case of Swiss citizens, the Swiss Federal Data Protection and Information Commissioner, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States.	For Business Personal Data, we use JAMS in the United States as our alternative dispute resolution provider. Such services are available in the United States. Information about JAMS is available at https://www.jamsadr.com/files/Uploads/Documents/Corporate-Fact-Sheet.pdf And information about the JAMS EU-U.S. Privacy Shield Program is available at https://www.jamsadr.com/eu-us-privacy-shield. In the case of Human Resources Personal Data, we cooperate with the panels established by European Data Protection Authorities and the Swiss Federal Data Protection and Information Commissioner, respectively.

What the Principles Require.	What we do.
Being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body.	We are subject to the investigatory and enforcement powers of the United States Federal Trade Commission (the "FTC"). You can learn more about the FTC's role in enforcement of the Privacy Shield at https://www.privacyshield.gov/article?id=OVERVIEW.
The possibility, under certain conditions, for the individual to invoke binding arbitration.	Under certain circumstances, you can invoke binding arbitration. We use JAMS in the United States as our alternative dispute resolution provider. Such services are available in the United States.
The requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.	We will disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
Its liability in cases of onward transfers to third parties.	If we transfer personal data to a third party and that transfer, or an act or omission by the third party, results in a violation of the Principles, we are liable for the transfer and/or the act or omission, even if it was the third party that committed the act or omission.
2. CHOICE	
An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.	You have the right to choose (opt out) whether your personal data is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by you. If you wish to opt out, all you need to do is contact us using the information in the section called "**How to Contact Us**." Applicable law allows certain exceptions to your ability to opt out, such as where we are parties to a contract that is still being performed, where law requires us to maintain information tow warranty claims, or otherwise. Where applicable law permits us to retain and continue to use such information and we do so, we will do so only to the extent permitted or required by law. If you contact us to opt out, we will explain the options available and comply with your request as required by the Principles and applicable law.
By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.	The above choice/opt-out doesn't apply where the sharing of your personal data is with a third party who is acting as our agent (such as our service providers who perform services that help us to run our business). We won't provide your personal data to a third party under these circumstances unless we have a contract in place with that third party that requires the third party to comply with the Principles.
For sensitive information (see the above definitions), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the	We will obtain your affirmative express consent (opt in) from you if we connect sensitive information and that information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice.

What the Principles Require.	What we do.
exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.	We also treat as sensitive any personal data received from a third party where the third party identifies and treats it as sensitive.
3. ACCOUNTABILITY FOR ONWARD TRANSFER	
To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third-party controller ceases processing or takes other reasonable and appropriate steps to remediate.	When we transfer personal data to a third party acting as a controller, we comply with the Notice and Choice Principles in the ways stated above. We also enter into contracts third-party controllers that provide that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the third-party controller will provide the same level of protection as the Principles and will notify us if the third party makes a determination that it can no longer meet this obligation. Those contracts provide that, when such a determination is made, the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.
To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization 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 Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.	Where we transfer personal data to a third party acting as an agent, (i) we transfer such data only for limited and specified purposes; (ii) we require (usually by contract) at least the same level of privacy protection as is required by the Principles; (iii) we take reasonable and appropriate steps to ensure that the agent effectively processes the personal data transferred in a manner consistent with the organization's obligations under the Principles; (iv) we require the agent to notify us 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 Principles; (v) upon notice, including under (iv), we take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) we will provide a summary or a representative copy of the relevant privacy provisions of our contract with that agent to the Department of Commerce upon request.
4. SECURITY	
Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.	We take reasonable and appropriate measures to protect personal data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction, taking into due account the risks involved in the processing and the nature of the personal data. We do this by adhering to internal policies and practices designed to meet these requirements.
5. DATA INTEGRITY AND PURPOSE LIMITATION	
Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently	We process personal data that we need in order to carry out our business. We only process personal information in a way that is compatible with the purposes for which we collected it or subsequently authorized by the data subject.

What the Principles Require.	What we do.
authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.	We take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. We adhere the Principles for as long as we retain the personal data.
Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of the paragraph above. This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the [Privacy Shield] Framework. Organizations should take reasonable and appropriate measures in complying with this provision.	Except as otherwise permitted by the Principles, we destroy or anonymize personal data after it no longer serves a purpose of processing as contemplated above and/or once a lawful basis for processing it ceases to exist.
6. 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, or has been processed in violation of the Principles, 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.	We give data subjects access to such personal data as we have that pertains to them and will help to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles If you wish to contact us to access your information, you can do so using the information in the section called "**How to Contact Us**." We reserve the right to limit such access and related activity where the burden or expense of providing access would be disproportionate to the risks to your privacy in the case in question, or where the rights of persons other than you would be violated.
7. RECOURSE, ENFORCEMENT AND LIABILITY	
Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:	
i. Readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;	For Business Personal Data, we use JAMS in the United States as our alternative dispute resolution provider. Such services are available in the United States. Information about JAMS is available at https://www.jamsadr.com/files/Uploads/Documents/Corporate-Fact-Sheet.pdf And information about the JAMS EU-U.S. Privacy Shield Program is available at https://www.jamsadr.com/eu-us-privacy-shield. If (1) your personal data was collected in a EU/EEA member country and/or Switzerland, and (2) you believe you have a claim concerning the collection, use, and retention of your personal data by LLamasoft, then you may contact JAMS to begin the process of opening a

What the Principles Require.	What we do.
	Data Privacy case. Your case must address an alleged breach of one or more of the Privacy Shield Principles. To see more information and to submit a claim please visit: https://www.jamsadr.com/file-an-eu-us-privacy-shield-claim In the case of Human Resources Personal Data, we cooperate with the panels established by European Data Protection Authorities or the Swiss Federal Data Protection and Information Commissioner, respectively.
ii. Follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of noncompliance; and	The corporate officer identified in our Privacy Shield certification (which you can see by looking us up at https://www.privacyshield.gov/list) is in charge of verifying that our attestations are true and that privacy practices have been implemented. That person has the necessary authority to carry out these functions. Additionally, our policies and procedures require our personnel to treat complaints and noncompliance as required by the Principles.
iii. Obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.	Our procedures, as contained in appropriate handbooks, job descriptions, policies, and notices announce our compliance with the Principles and provide for appropriate sanctions for noncompliance by our employees and agents.
Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State (or Swiss) authorities through the Department. Organizations that have chosen to cooperate with DPAs (or, in the case of Swiss data subjects, Swiss Federal Data Protection and Information Commissioner), including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.	We will, and we will cause our independent recourse mechanisms to, promptly comply with any requests by any applicable government agency for information relating to the Privacy Shield and we will respond to complaints by EU Member State or Swiss authorities as required by the Principles.
Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.	“Annex I” contains the terms under which Privacy Shield certifying organizations are obliged to arbitrate claims as required by the Recourse, Enforcement, and Liability Principles. Where an individual has invoked binding arbitration by delivering notice the required notice, we will arbitrate as required by the terms in Annex I. You can see Annex I for yourself if you like at (for the EU-U.S. Privacy Shield) EU - US Privacy Shield ANNEX 1 or (for the Swiss-U.S. Privacy Shield) Swiss - US Privacy Shield ANNEX 1
In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield	We take responsibility for our agents’ compliance with the Principles for all personal data that we receive under the Privacy Shield. We require our agents, by contract or

What the Principles Require.	What we do.
and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.	otherwise, to comply with the Principles when processing such personal data. We will be and remain liable for such processing unless we prove that we are not responsible for the event giving rise to the damage.
When an organization becomes subject to an FTC or court order based on noncompliance, the organization shall make public any relevant Privacy Shield related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs and with the Swiss Federal Data Protection and Information Commissioner for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State and Swiss authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.	When we become subject to an FTC or court order based on noncompliance, we will make public any relevant Privacy Shield -related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements.

How to Contact Us

You can contact us using the following information

Privacy Office

LLamasoft, Inc. (a Coupa company)

E-Mail: GDPR@coupa.com