

The EU-US and Swiss-US Privacy Shield are frameworks for the transatlantic exchange of personal data for commercial purposes between the European Union, (including Liechtenstein, Norway and Iceland) and Switzerland in to the United States. One of its purposes is to enable US companies to more easily receive personal data from EU entities under EU privacy laws meant to protect European Union and Swiss citizens. The EU-US and Swiss-US Privacy Shield frameworks replace the US-EU and US-Swiss Safe Harbor Privacy Frameworks which were declared invalid by the European Court of Justice in October 2015.

All Zift Solutions employees who handle Personal Data from the European Union and Switzerland are required to comply with the Principles.

Capitalized terms are defined in Section 12 of this Policy.

1. Scope

Important Notice to Non-U.S. Residents

In order to satisfy the requirement under European Union (“EU”) and Swiss laws that adequate protection be given to personal data transferred from EU member countries and Switzerland to the United States, Zift Solutions complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from European Union and Switzerland to the United States, respectively. Zift Solutions has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. However, it is important to note that the Website is operated in the United States. If you are located outside of the United States, please be aware that any Information you provide to us will be transferred to the United States. By using the Website, participating in any of our services, and/or providing us with your information.

To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>.

2. Type of data processed

Zift Solutions, sells Channel as a Service (CHaaS) solutions that our customers use to manage their partner relationships. In providing these tools, Zift Solutions processes data our customers enter into our products or instruct us to process on their behalf. Zift Solutions customers decide what to enter. Zift Solutions generally has no knowledge about what is being stored. However, our understanding is that typically the information includes personal information required for business purposes only, about our customers, their partners, and their partners’ customers, prospects and/or sales leads (“Data Subjects”) (e.g. names, business addresses, work phone numbers, work e-mail addresses etc.).

3. Purposes

Zift Solutions processes Customer Data pursuant to our subscription agreement. Our products are deployed on Software As a Service (SaaS) platform and customers will also engage us for professional services and customer support. To fulfil our contractual obligations, Zift

Solutions may access Customer Data to provide services, to correct and address technical or service problems, or to follow instructions of the customer who submitted the data, or in response to contractual requirements. Zift Solutions will not sell, rent, exchange or share your personal information to non-agent third parties for purposes materially different from those for which the data was provided. If this practice should change in the future we will update this policy accordingly, identify all non-agent third parties, and provide individuals with opt-out or opt-in (if applicable) choice.

4. Third Parties who may receive personal data (Onward Transfer)

Zift Solutions may employ and contract with third-party service providers and other entities to assist in providing our services to customers by performing certain tasks on our behalf. These third-party providers may offer customer support, data storage services (data centers), or technical operations. Zift Solutions maintains contracts with these third parties restricting their access, use and disclosure of personal data in compliance with our Privacy Shield obligations. These third parties may access, process, or store personal data in the course of providing their services. Unless we tell you differently, our Agents do not have any right to use Personal Information or other information we share with them beyond what is necessary to assist us. You hereby consent to our sharing of Personal Information with our Agents. We may be liable for the appropriate onward transfer of EU and Swiss personal data to third parties.

5. Compelled disclosure

Zift Solutions may be required to disclose collected information in order to (i) respond to investigations, court orders or legal process, (ii) to investigate, prevent or take action regarding illegal activities, suspected fraud, potential threats to the physical safety of any person, (iii) violations of Zift Solutions' terms of service, or (iv) as otherwise required by law. Note that we may be required to share personal data of EU and/or Swiss individuals in response to lawful requests by public authorities including to meet national security and law enforcement requirements.

6. Data Integrity & Security

Zift Solutions maintains commercially reasonable safeguards to maintain the accuracy, integrity and security of Personal Data.

Security: Zift Solutions takes reasonable and appropriate precautions, including administrative, technical, personnel, and physical measures, to safeguard Personal Data against loss, misuse, theft, and unauthorized access, disclosure, alteration, and destruction. Zift Solutions security policies, operating procedures, and technical controls, where applicable, generally adhere to commonly accepted standards for security of networks, infrastructure, applications, and data.

Data Integrity: Zift Solutions limits its collection of Personal Data to that which is relevant for the intended business and legal purposes. Zift Solutions does not use the data in a way that is incompatible with the purposes for which it was collected or subsequently authorized by the individual. To the extent necessary for those purposes, Zift Solutions takes reasonable steps to ensure that Personal Data is reliable for its intended use, accurate, complete, and current.

7. **Your rights to access, to limit use and to limit disclosure**

If you are an individual based in the EU and our product holds your personal data, you may request access to your personal data. You also have the right to update, correct or delete, or to limit the use or disclosure of, your personal data. Zift Solutions acknowledges the right of EU and Swiss individuals to access their personal information stored in the US.

Individuals wishing to view, update, delete, or supplement their personal data may do so by contacting the business that provided Zift Solutions your personal data directly to make your requests, or alternatively you can contact us directly at privacy@ziftsolutions.com.

If you contact us directly, you will need to provide the name of the Zift Solutions customer who submitted your personal data to our product. We will refer your request to that customer and will support them as needed in responding to your request.

8. **Inquiries and complaints**

In compliance with the EU-US and Swiss-US Privacy Shield Principles, Zift Solutions commits to resolve complaints about your privacy and our collection or use of your personal information. EU individuals with inquiries or complaints regarding this Privacy Shield policy should first contact Zift Solutions at:

Zift Channel Solutions, Inc. 30 Montgomery St, Suite 1210, Jersey City, NJ 07302, USA, or call us at +1 (919) 794-8385, or email us at privacy@ziftsolutions.com.

Zift Solutions has further committed to refer unresolved Privacy Shield complaints to Council of Better Business Bureaus (CBBB), an alternative dispute resolution provider located in the United States. 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 or visit <https://www.bbb.org/EU-privacy-shield/for-eu-consumers> for more information or to file a complaint. The services of CBBB are provided at no cost to you.

9. **US Federal Trade Commission enforcement**

Zift Solutions is subject to the investigatory and enforcement authority of the United States Federal Trade Commission (FTC).

10. **Binding Arbitration**

Finally, and under limited circumstances, individuals with unresolved privacy complaints can invoke a binding arbitration option before a Privacy Shield Panel. You may have the option to select binding arbitration for the resolution of your complaint under certain circumstances, provided you have taken the following steps: (1) raised your complaint directly with Zift Solutions and provided us the opportunity to resolve the issue; (2) made use of the independent dispute resolution mechanism identified under the **Inquiries and complaints** paragraph; and (3) raised the issue through the relevant data protection authority and allowed the US Department of Commerce an opportunity to resolve the complaint at no cost to you. For more information on binding arbitration, see US Department of Commerce's Privacy Shield Framework: Annex I (Binding Arbitration).

11. Changes to Zift Solutions Privacy Policy

This Policy may be amended from time to time, consistent with the Principles and applicable data protection and privacy laws and principles. Zift solutions will notify Data Subjects if it makes changes that materially affect the way it handles Personal Data previously collected, and will allow individuals to choose whether Personal Data supplied by them may be used in any materially different manner. We may also place a prominent notice on our website in regards to material changes to our privacy policy.

12. Definitions

Capitalized terms in this Privacy Policy have the following meanings:

"Zift Solutions" means Zift Channel Solutions, Inc and its affiliates and subsidiaries to which the Principles apply. A list of the entities covered by the Principles is available at www.privacyshield.gov.

"Data Subject" means an identified or identifiable natural living person. An identifiable person is one who can be identified, directly or indirectly, by reference to a name, or to one or more factors unique to his or her personal physical, psychological, mental, economic, cultural or social characteristics. For Customers residing in Switzerland, a Data Subject also may include a legal entity.

"Customer" means a prospective, current, or former partner (distributor or reseller), vendor, supplier, customer, or client of Zift Solutions from Europe. The term also shall include any individual agent, employee, representative, customer, or client of a Customer of Zift Solutions where Zift solutions has obtained his or her Personal Data from such Customer as part of its business relationship with the Customer.

"Europe" or "European" refers to a country in the European Economic Area which, for the purposes of this Policy, includes Switzerland, Norway, Liechtenstein and Iceland.

"Legal Department" means Zift Solutions legal department who can be contacted by phone on at +1 (919) 794-8385 or email at privacy@ziftsolutions.com.

"Personal Data" as defined under the European Union Directive 95/46/EC and the Swiss Federal Data Protection Act of 19 June 1992 means data that personally identifies or may be used to personally identify a person. Personal Data does not include data that is de-identified, anonymous, or publicly available. For Switzerland, the term "person" includes both a natural person and a legal entity, regardless of the form of the legal entity.

"Third Party" means any individual or entity that is neither Zift Solutions nor an Zift Solutions employee, agent, contractor, or representative.

Last Update: March 2018