Data Privacy Framework Policy

Current Version: 8 May 2025

EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S

Ziflow Inc.(“Ziflow”, “we”, “our” or “us”) has subscribed to the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S (collectively, “DPF”). Ziflow adheres to the EU-U.S. and the UK Extension. Data Privacy Framework Principles including the Supplemental Principles, (collectively, the “DPF Principles”) for Personal Data received from entities in the European Economic Area (the “EEA”), the United Kingdom (“UK”).

This Ziflow Data Privacy Framework Policy (“DPF Policy”) and the Ziflow Privacy Policy (“Privacy Policy”) describe the privacy practices that we implement for Personal Data received from the EEA or UK in reliance on the DPF. This DPF Policy uses terms which are defined in the Privacy Policy.

If there is any conflict between the terms in this DPF Policy and the DPF Principles, the DPF Principles shall govern to the extent of the conflict. To learn more about the DPF program visit https://www.dataprivacyframework.gov/, and to view our certification, please visit https://www.dataprivacyframework.gov/list.

DPF Principles

Notice and Choice

Our Privacy Policy describes how we use Personal Data we receive from different sources. This DPF Policy describes how we process Personal Data covered by the DPF.

Ziflow may act as an agent for you in relation to the Personal Data that you provide or make available to Ziflow. In its role as a controller and as required by applicable law, Ziflow generally offers individuals in the EU and UK (together: “EEA/UK Consumers”) the opportunity to choose whether their Personal Data may be (i) disclosed to third-party controllers or (ii) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant EEA/UK/CH Consumer. To the extent required by the DPF Principles, Ziflow obtains opt-in consent for certain uses and disclosures of sensitive data. EEA/UK/CH Consumers may contact Ziflow as indicated below regarding the Ziflow’s use or disclosure of their Personal Data. Unless Ziflow offers EEA/UK/CH Consumers an appropriate choice, Ziflow uses

Personal Data only for purposes that are materially the same as those indicated in this Policy.

Data Integrity and Purpose Limitation

We only collect Personal Data that is relevant to providing our Services. We process Personal Data compatible with us providing the Services or as otherwise notified to you. We take reasonable steps to ensure that the Personal Data received under the DPF is needed for Ziflow's Services, accurate, complete, and current.

Accountability for Onward Transfers

This Policy and the Privacy Policy describe how Ziflow shares Personal Data.

Except as permitted or required by applicable law and in accordance with Ziflow's role as a controller or processor, Ziflow provides EEA/UK/CH Consumers with an opportunity to opt out of sharing their Personal Data with third-party controllers. Ziflow requires third-party controllers to whom it discloses the Personal Data of EEA/UK/CH Consumers to contractually agree to (a) only process the Personal Data for limited and specified purposes consistent with the consent provided by the relevant EEA/UK/CH Consumer, (b) provide the same level of protection for Personal Data as is required by the DPF Principles, and (c) notify Ziflow and cease processing Personal Data (or take other reasonable and appropriate remedial steps) if the third-party controller determines that it cannot meet its obligation to provide the same level of protection for Personal Data as is required by the DPF Principles.

Ziflow may disclose Personal Data to trusted third parties as indicated in the Privacy Policy without offering an opportunity to opt out. Ziflow requires that its agents and service providers that have access to Personal Data within the scope of this DPF Policy provide the same level of protection as required by the DPF Principles. We shall remain liable under the Principles if our agents and service providers process such personal information in a manner inconsistent with the Principles, unless we prove that we are not responsible for the event giving rise to the damage.

We may also need to disclose Personal Data in response to lawful requests by public authorities, for law enforcement or national security reasons, or when such action is necessary to comply with a judicial proceeding or court order, or when otherwise required by law. We do not offer an opportunity to opt out from this category of disclosure.

Data Security

We use reasonable and appropriate physical, electronic, and administrative safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information.

Access to Personal Data

Our Privacy Policy explains how you may access and/or submit requests to review, correct, update, suppress, or delete Personal Data. You can ask to review and correct Personal Data that we maintain about you by sending a written request to privacy@ziflow.com. We may limit or deny access to Personal Data where providing such access is unreasonably burdensome, expensive under the circumstances, or as otherwise permitted by the DPF Principles.

When Ziflow acts on behalf of its Users, Ziflow will assist Users in responding to individuals exercising their rights under the DPF Principles.

DPF Recourse and Enforcement

In compliance with the DPF Principles, Ziflow Inc. commits to resolve complaints about our collection or use of your personal information. EU and UK individuals with inquiries or complaints regarding our DPF Policy should first contact Ziflow Inc. at:

privacy@ziflow.com or by filling out the form on our Contact page.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Ziflow commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

Under certain conditions, more fully described on the DPF Principles website (https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction), you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

Ziflow is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (“FTC”).

Changes to this DPF Policy

This DPF Policy may be changed from time to time, consistent with the requirements of the DPF and in accordance with the process described in the

Privacy Policy. You can determine when this DPF Policy was last revised by referring to the “CURRENT VERSION” date at the top of this page.