Data Processing Addendum

Current Version: 11 March 2024

The purpose of this Data Processing Addendum ("DPA") is to set out Ziflow's obligations relating to the Personal Data processed by it in the provision of the Service to the Customer pursuant to the Agreement.

1. Definitions

Defined terms used in the Master Subscription Agreement shall have the same meaning where used in this DPA unless otherwise defined herein.

Appropriate Safeguards means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time including the EU SCCs and UK Addendums.

Applicable Law means as applicable and binding on Customer, Ziflow and/or the Services:

i. any law, statute, regulation, by-law or subordinate legislation in force from time to time to which a party is subject;
ii. any court order, judgment or decree;
iii. or any direction, policy, rule, or order that is made or given by any regulatory body having jurisdiction over a party.

Controller means the entity which determines the purposes and means of the Processing of Personal Data.

Customer Content means electronic files, logos, data and information uploaded under Customer's account to the Service, whether directly or through the API (i.e. the programming interface to the Service).

Data Protection Laws means

iv. the General Data Protection Regulation (EU) 2016/679 and any applicable national implementing laws as amended from time to time;
v. the UK Data Protection Laws; and
vi. all laws about the processing of personal data and privacy applicable to the processing of Protected Data pursuant to this DPA.

Data Subject means the identified or identifiable person to whom Personal Data relates.

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws.

EU SCCs means Module 2 of the Controller to Processor Standard Contractual Clauses approved by the European Commission pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (as amended and updated from time to time).

Personal Data means any information relating to

vii. an identified or identifiable natural person and,
viii. an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws.

Personal Data Breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data.

Processor means the entity which Processes Personal Data on behalf of the Controller.

Processing means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (and related terms such as process have corresponding meanings).

Processing Instructions has the meaning given to that term in clause 3.b.

Protected Data means Personal Data submitted to the Service (excluding any in Customer Content) or otherwise provided to Ziflow by the Customer in pursuance of use of the Service by Customer.

Sub-Processor means another Processor engaged by Ziflow for carrying out processing activities in respect of the Protected Data.

Supervisory Authority means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

UK Data Protection Laws means the Data Protection Act 2018 and UK GDPR.

UK GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

UK Addendum means the International Data Transfer Addendum issued by the Information Commissioner's Officer under Section 119A of the Data Protection Act 2018, effective from 21 March 2022.

Working Day means Monday to Friday inclusive excluding bank and public holidays in the UK.

2. Roles and obligations

a. The parties agree that, for the Protected Data, Customer shall be the Controller and Ziflow shall be the Processor.
b. Ziflow shall process the Protected Data in compliance with:
    i. the obligations of Processors under Data Protection Laws; and
    ii. the terms of this DPA.
c. Customer, is required to ensure all Personal Data it provides to Ziflow for use in connection with the Service shall be collected and transferred to Ziflow or submitted to the Service in

accordance with Data Protection Laws. For the avoidance of doubt, it shall be Customer's responsibility to

iii. ensure the terms of use it supplies to the Data Subjects of the Protected Data comply with Data Protection Laws including in particular any fair processing information requirements relating to the processing of the Protected Data by Ziflow; and
iv. to ensure it has a legal basis for the processing of the Protected Data by Ziflow.

3. Instructions

a. Customer as Controller is required, in its use of the Service, to Process Protected Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Protected Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Protected Data and the means by which Customer acquired Personal Data.
b. Insofar as Ziflow processes Protected Data, Ziflow:
    i. shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with Customer's documented instructions from time to time and in accordance with Schedule 1 (Data Processing Particulars), as updated from time to time ("Processing Instructions"); and
    ii. shall inform Customer if Ziflow is aware of a Processing Instruction that, in its opinion, infringes Data Protection Laws.

4. Technical and organisational measures

Security Measures. Ziflow:

i. implements and maintains reasonable security measures appropriate to the nature of the Protected Data including, without limitation, technical, physical, administrative, and organizational controls, designed to maintain the confidentiality, security, and integrity of the Protected Data;
ii. implements and maintains industry-standard systems and procedures for detecting, preventing, and responding to attacks, intrusions, or other systems failures and regularly tests, or otherwise monitors the effectiveness of the safeguards' key controls, systems, and procedures;
iii. designates an employee or employees to coordinate implementation and maintenance of its Security Measures (as defined below); and
iv. identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Protected Data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of safeguards in place to control these risks (collectively, Security Measures). Ziflow's security policy is located here and will not be materially degraded during the term of all orders under the Agreement: https://www.ziflow.com/security.

5. Sub processors and staff

a. Ziflow has appointed Sub-Processor(s) under a written contract containing materially equivalent obligations to those in this Data Processing Addendum. Full details of current Sub-Processors and can be found here: https://www.ziflow.com/sub-processors.
b. Ziflow shall ensure that all of its personnel and contractors processing Protected Data are subject to a binding written contractual obligation with Ziflow or are under professional obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case Ziflow shall, where practicable and not prohibited by Applicable Law, notify Customer of any such requirement before such disclosure) Ziflow is responsible for the acts, omissions, willful misconduct or negligence of sub-processors, staff and agents to include employees, contractors and temporary staff.
c. Ziflow may change Sub-Processor(s) form time to time. It is the responsibility Customer to regularly check the list of Sub-Processors published here: https://www.ziflow.com/sub-processors for changes. The Customer has twenty days (from date of the change in Sub-Processor) to object to the change in Sub-Processor on reasonable and objectively justifiable grounds. If Customer objects to the change in Sub-Processor, Ziflow will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid Processing of the Protected Data by the objected to new Sub-Processor. If Ziflow is unable to make available such change within a reasonable period of time, Customer may, by written notice, terminate the Service which cannot be provided by Ziflow without the use of the objected to new Sub-Processor. Ziflow will provide a refund of any prepaid fees covering the remainder of the term of such Service following the effective date of termination with respect to such terminated Service.

6. Data subject request and assistance

a. Ziflow shall promptly refer all Data Subject Requests it receives to Customer as appropriate (wherever practicable within two Working Days of receipt of the request).
b. Ziflow shall provide such assistance to Customer as Customer reasonably requires (taking into account the nature of processing and the information available to Ziflow) to ensure compliance with each party's obligations under Data Protection Laws with respect to:
    i. Data Subject Requests;
    ii. security of processing;
    iii. data protection impact assessments (as such term is defined in Data Protection Laws);
    iv. prior consultation with a Supervisory Authority regarding high risk processing; and
    v. notifications to the Supervisory Authority and/or communications to Data Subjects by Customer in response to any Personal Data Breach and for the avoidance of doubt Ziflow must promptly notify Customer in writing of any communications received by it from Data Subjects or Supervisory Authorities relating to the Protected Data without responding to either of the same unless it has been expressly authorised to do so by Customer.
c. Ziflow shall be entitled to reimbursement of its reasonable costs for providing such notifications and assistance pursuant to sub-clause 6.a. above.

7. Overseas transfers

a. To the extent required under Data Protection Laws, Ziflow shall ensure that any transfers (and any onward transfers) of Protected Data under this DPA from the European Union, the

European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws of the foregoing territories (Third Countries), are effected by way of Appropriate Safeguards.

b. Where Ziflow processes Protected Data in non-EEA/UK countries, Ziflow shall comply with the EU SCCs which shall be entered into and incorporated into this DPA by this reference and completed as follows:
    i. Module 2 (Controller to Processor) will apply where Customer is a controller of Protected Data and Ziflow is a processor of Protected Data; Module 3 (Processor to Processor) will apply where Customer is a processor of Protected Data and Ziflow is a processor of Protected Data. For each Module, where applicable:
    ii. in Clause 7, the optional docking clause will apply;
    iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 5 of this DPA;
    iv. in Clause 11, the optional language will not apply;
    v. in Clause 12, any claims brought under the EU SCCs shall be subject to the terms and conditions set forth in the Master Subscription Agreement. In no event shall any party limit its liability with respect to any data subject rights under the EU SCCs.
    vi. in Clause 17, Option 1 will apply, will be governed by English law;
    vii. in Clause 18(b), disputes shall be resolved before the courts of England;
    viii. **Annex I** of the EU SCCs shall be deemed completed with the information set out in **Schedule I** to this DPA; and
    ix. **Annex II** of the EU SCCs shall be deemed completed with the information set out in **Schedule II** to this DPA.
c. Nothing in the interpretations in this Section 7 is intended to conflict with either Party's rights or responsibilities under the EU SCCs or UK Addendum and, in the event of any such conflict, the EU SCCs or the EU SCCs with UK Addendum (as applicable) shall prevail.
d. To the extent any export from or processing of Protected Data outside the United Kingdom is subject to UK Data Protection Laws, then Ziflow shall comply with the EU SCCs and the UK Addendum which shall be entered into and incorporated into this DPA by this reference. The EU SCCs shall be completed as set out above in Section 7b (i)-(ix) of this DPA and shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Protected Data. Tables 1-3 of Part One of the UK Addendum shall be deemed completed with the information set out in Schedule I and Schedule II to this DPA. For the purposes of Table 4 of Part One of the UK Addendum, Ziflow may end the UK Addendum when it changes. If neither the EU SCCs or the UK Addendum with EU SCCs applies, then the Parties shall cooperate in good faith to implement appropriate safeguards for transfers of such Protected Data as required or permitted by the UK Data Protection Laws without undue delay.
e. Details of onward transfers by Ziflow to, and of the Appropriate Safeguards in place with, Sub-processors can be found here: https://www.ziflow.com/sub-processors

8. Records and audits

a. Ziflow shall maintain written records of all categories of processing activities carried out on behalf of Customer.
b. Ziflow shall make available to Customer such information as is reasonably necessary to demonstrate its compliance with the obligations of Processors under Data Protection Laws, and shall allow for and contribute to audits, including inspections, by Customers (or another auditor mandated by Customer) for this purpose, subject to Customer:
    i. giving Ziflow at least 30 days' advance notice of such information request, audit and/or inspection being required;

ii. the parties mutually agreeing the scope, timing, and duration of the audit in addition to a reimbursement rate Ziflow's time and effort in co-operating with such audit, for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Ziflow; and

iii. ensuring that all information obtained or generated by Customer or its or its mandated auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law). Customer shall, and shall where appropriate procure that Customer, provide a copy of such information and audit reports to Ziflow following an inspection or audit pursuant to this clause 8.

9. Breach notification

In respect of any Personal Data Breach involving Protected Data, Ziflow shall without undue delay and in any event within 48 hours of becoming aware of the Personal Data Breach:

i. notify Customer of the Personal Data Breach; and
ii. so far a possible without prejudicing the continued security of the Protected Data or any investigation into the Personal Data Breach, provide Customer with details of the Personal Data Breach.

10. Deletion or return of protected data

a. Customer may extract the Protected Data prior to or on termination in accordance with the Ziflow transition assistance policy located at http://www.ziflow.com/transition-assistance-policy.
b. Upon termination Ziflow will destroy any Protected Data remaining on the Service.
c. If after termination continued storage by Ziflow of any Protected Data is required by Applicable Law, Ziflow shall inform Customer of any such requirement and the period during which it is required to be stored. Ziflow shall not process such Protected Data except to the extent required by Applicable Law. Such Protected Data shall remain subject to the terms of this DPA.

11. Liability

a. If a party receives a compensation claim from a person (including but not limited to a Data Subject) relating to processing of Protected Data processed by Ziflow under the Contract, it shall promptly provide the other party with notice and full details of such claim. Customer shall make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of Ziflow.
b. This clause 11 does not affect the liability of Ziflow to any Data Subject or Supervisory Authority pursuant to a claim made directly against Ziflow by either of them.
c. As between Ziflow and Customer liability for all loss, damage, claims, fines or penalties ("Losses") arising out of any breach of this DPA including for any Losses arising out of a Personal Data Breach, shall be governed by the limitations of liability and remedies for loss of data as set out in the Contract.

d. Customer acknowledges that it is not permitted to include Personal Data in Customer Content and Ziflow excludes all liability for any claims, penalties, fines, damages or costs arising in respect of Personal Data in Customer Content including from any Personal Data Breach involving Personal Data in Customer Content.

SCHEDULE I: DATA PROCESSING PARTICULARS

1. Subject-matter of processing:

Identification and contact data of users of the Service; customer relationship management and payment management

2. Duration of the processing:

Subject to Clause 10 of this DPA, Ziflow will Process Protected Data for the duration of the Customer's subscription to the Service, unless otherwise agreed upon in writing.

3. Nature and purpose of the processing:

To use the Protected Data for the purpose of providing the Services and as otherwise detailed in the Contract, and as further instructed by Customer in its use of the Services.

4. Type of Personal Data:

The use of the Service requires no Personal Data to be submitted by the Customer in Customer Content and Customer must not include Personal Data in Customer Content which is input into the Services. Customer may only submit Personal Data to the Services in relation to administration of users of the Service which includes, the following categories of Personal Data:

First and last name

Title

Position

Employer

Contact information (company, email, phone, physical business address)

Connection data

Localisation data

Special Category Data: None

5. Categories of Data Subjects:

The Personal Data processed by Ziflow in relation to the Service relates only to the following categories of data subjects: Employees, agents, advisors, freelancers of Customer (who are natural persons) and who are authorized by Customer to use the Service

6. Processing Instructions

To use the Protected Data for the purpose of administering and managing authorised users of the Service and for payment and customer relationship management purposes and as otherwise instructed in writing from time to time.

SCHEDULE II: SECURITY MEASURES

Details of the security measures can be found here: https://www.ziflow.com/security.