Ecosystem Data Processing Addendum

This Ecosystem Data Processing Addendum **("DPA")**, reflects the parties' agreement with respect to the terms governing the Processing of Personal Data under the Terms of Service for Customers and Terms of Service for Vendors **(the "Agreement")**. This DPA is part of the Agreement and is effective upon its incorporation into the Agreement.

The purpose of the DPA is to ensure that processing of Personal Data as defined below is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Data are processed. Other capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement. This DPA applies in respect of processing that is carried by Zapflow in the role of the Processor as defined below.

The term of this DPA shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

This DPA also includes:

- Appendix 1 A description of the technical and organizational security measures implemented by the Processor as referenced.
- Appendix 2 List of Sub-Processors.

1. Definitions

"Controller" means Zapflow in respect of processing Personal Data in Customer Information or Vendor Information as defined in the Agreement

"Data Protection Law" means EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "GDPR") and any other applicable European or foreign data protection laws as amended.

"Data Subject" means the individual to whom Personal Data relates.

"EEA" means the European Economic Area,

"GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data.

"Instruction" means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action regarding Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

“Personal Data” means any information relating to an identified or identifiable natural person where such information is contained within Customer Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

”Processor” means Zapflow in respect of processing Personal Data submitted by Customer or Vendor and processed by Zapflow within the Service Ecosystem, however excluding Personal Data in Customer Information or Vendor Information that is processed by Zapflow as the Controller.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, or erasure of Personal Data.

“Standard Contractual Clauses” means the clauses pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

2. Details of the Processing

1. **Categories of Data Subjects.** Customer and Vendor are controllers of the Personal Data that Zapflow processes as the Processor in the Service Ecosystem. Zapflow does not have precise knowledge of categories of Data Subjects, however, it assumes that Customer or Vendor may submit such categories of Data Subjects as employees, contractors, collaborators, customers, prospects, suppliers, and subcontractors of Customer or Vendor.
2. **Types of Personal Data.** Contact information such as name, address, email-address, phone numbers and other Personal Data submitted, stored, sent, or received in respect of Data Subjects that Zapflow processes as the Processor. Vendors and Customer shall not submit any special categories of Personal Data, as defined under GDPR.
3. **Subject-Matter and Nature of the Processing.** The subject-matter of Processing of Personal Data by Processor is the provision of the Service Ecosystem to Customers/Vendors that involves the Processing of Personal Data by Zapflow acting as the Processor.
4. **Purpose of the Processing.** Personal Data will be Processed for purposes of providing the Service Ecosystem set out and otherwise agreed to in the Agreement.
5. **Duration of the Processing.** Personal Data will be Processed for the duration of the Agreement, subject to Section 4 of this DPA.

3. Responsibility of the Customer / Vendor

Within the scope of the Agreement and use of the Service Ecosystem, Customer /Vendor shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. Instructions shall initially be specified in the Agreement and may, from time to time thereafter, be amended, amplified, or replaced by Customer/Vendor in separate written instructions (as individual instructions). For the avoidance of doubt, Customer's/Vendor's instructions for the Processing of Personal Data shall comply with the Data Protection Law.

Customer/Vendor shall inform Processor without undue delay and comprehensively about any errors or irregularities related to instructions for Processing of Personal Data.

4. Obligations of Processor

1. **Compliance with Instructions.** Processor shall collect, process, and use Personal Data only within the scope of Customer's/ Vendor's Instructions. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under any applicable Data Protection Law, Processor will (i) promptly notify the Customer/Vendor of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Customer/Vendor issues new instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Customer/ Vendor under the Agreement for any failure to perform the applicable services until the Customer/Vendor issues new instructions regarding the Processing.
2. **Security.** Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, described under Appendix 1.
3. **Confidentiality.** Processor shall ensure that any personnel and sub-processors whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the above-entitled activities.
4. **Personal Data Breaches.** Processor will notify the Customer/Vendor without undue delay after it becomes aware of any Personal Data Breach affecting any Personal Data. At the Customer's/ Vendor's request, Processor will promptly provide the Customer/Vendor with all reasonable assistance necessary to enable the Customer/Vendor to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Customer/Vendor is required to do so under the Data Protection Law.
5. **Data Subject Requests.** Processor will provide reasonable assistance, including by appropriate technical and organizational measures and considering the nature of the Processing, to enable Customer/Vendor to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection

Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Customer/Vendor and will advise Data Subjects to submit their request to the Customer/Vendor. Customer/Vendor shall be solely responsible for responding to any Data Subjects' requests. Customer/Vendor shall reimburse Processor for the costs arising from this assistance.

6. **Sub-Processors.** Processor shall be entitled to engage sub-Processors to fulfill Processor's obligations defined in the Agreement only with Customer's/Vendor's 's written consent. For these purposes, Customer/Vendor consents to the engagement as sub-Processors of Processor's affiliated companies and the third parties listed in Appendix 2. For the avoidance of doubt, the above authorization constitutes Customer's/Vendor's prior written consent to the sub-Processing by Processor for purposes of Clause 11 of the Standard Contractual Clauses. If the Processor intends to instruct sub-Processors other than the companies listed in Appendix 2, the Processor will notify the Customer/Vendor thereof in writing (email to the email address(es) on record in Processor's account information for Customer/Vendor is sufficient) and will give the Customer/Vendor the opportunity to object to the engagement of the new sub-Processors within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the Customer/Vendor proves that significant risks for the protection of its Personal Data exist at the sub-Processor). If the Processor and Customer/Vendor are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party. Customer/Vendor shall receive a refund of any prepaid but unused fees for the period following the effective date of termination. Where Processor engages sub-Processors, Processor will enter into a contract with the sub-Processor that imposes on the sub-Processor the same obligations that apply to Processor under this DPA. Where the sub-Processor fails to fulfill its data protection obligations, Processor will remain liable to Customer/Vendor for the performance of such sub-Processors obligations.
7. **Data Transfer outside EEA.** The provision 6 of this Section 4 shall apply if the Processor engages a sub-Processor in a country outside the European Economic Area ("EEA") not recognized by the European Commission as providing an adequate level of protection for personal data. If, in the performance of this DPA, Zapflow transfers any Personal Data to a sub-processor located outside of the EEA, Zapflow shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place. . Customer/Vendor acknowledges and agrees that, relating to the performance of the services under the Agreement, Personal Data will be transferred to Zapflow Ltd in Finland and to sub-Processors within the EEA.
8. **Deletion or Retrieval of Personal Data**. Other than to the extent required to comply with Data Protection Law, following termination or expiry of the Agreement or written request from the Customer/Vendor, Processor will delete all Personal Data (including copies thereof) processed pursuant to this DPA. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing. Customer/Vendor shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within a period set by Processor, the reasonable measures to return data or to delete stored

data. Any additional cost arising relating to the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Customer/Vendor.

5. Audits

Customer/Vendor may, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organizational measures taken by Processor. For such purpose, Customer/Vendor may, e.g., a) obtain information from the Processor and b) upon reasonable and timely advance agreement, during regular business hours and without interrupting Processor’s business operations, conduct an on-site inspection of Processor’s business operations or have the same conducted by a qualified third party which shall not be a competitor of Processor.

Processor shall, upon Customer’s/Vendor’s written request and within a reasonable period of time, provide Customer/Vendor with information necessary for such audit, to the extent that such information is not a Processors trade secret, is within Processor’s control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party. Processor shall have the right to limit access to certain business and security critical information and instead give a summary overview of such information. Any auditor conducting the audit shall executive a non-disclosure agreement binding all auditors as well as the companies they represent.

Appendix 1- Security Measures

Zapflow currently observes the security practices described in this Appendix 1. Notwithstanding any provision to the contrary otherwise agreed to by Processor, Zapflow may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

Access Control

1. Preventing Unauthorized Product Access

Outsourced processing: Zapflow hosts its Service Ecosystem with outsourced cloud infrastructure provider. Additionally, Zapflow maintains contractual relationships with vendors in order to provide the Service in accordance with this Data Processing Addendum. Zapflow relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Zapflow hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: Customers and Vendors who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Zapflow’s products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user’s permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

2. Preventing Unauthorized Product Use

Zapflow implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Zapflow implemented a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in Zapflow’s source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: Zapflow maintains relationships with industry recognized penetration testing service providers for penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

3. Limitations of Privilege & Authorization Requirements

Product access: A subset of Zapflow’s employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” requests for access; all such requests are logged. Employees are granted access by role. Employee roles are reviewed at least once every six months.

Transmission Control

In-transit: Zapflow makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Zapflow products. Zapflow’s HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Zapflow stores user password hashes following policies that follow industry standard practices for security.

Input Control

Detection: Zapflow designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Zapflow personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Zapflow maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Security, operations, or support personnel investigates suspected and confirmed security incidents; and appropriate resolution steps are identified and documented. For any confirmed incidents, Zapflow will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Zapflow becomes aware of unlawful access to Customer Data stored within its products, Zapflow will: 1) notify the affected Customers of the incident; 2) provide a description of the steps Zapflow is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Zapflow deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Zapflow selects, which may include via email or telephone.

Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99 % uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Zapflow's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Zapflow operations in maintaining and updating the product applications and back-end while limiting downtime.

APPENDIX 2 – LIST OF SUB-PROCESSORS

We use a small selection of trusted 3rd-party data sub-processors to deliver our services.

Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 89109-5210, USA

All personal data is stored and processed in European data centers of our sub-processor Amazon Web Services (AWS). AWS is GDPR-compliant and is ISO 27001, 27017 and 27018 certified. ISO 27018 is a code of conduct for the protection of personal data in the cloud. It is based on the ISO 27002 information security standard and serves as a guideline for the implementation of ISO 27002-controls that apply to personal data that uniquely identifies a person in the public cloud. The standard provides additional controls and guidelines for the protection requirements of personal data that are not taken into account by the current controls of ISO 27002.

By complying with this standard, AWS has a system of control mechanisms that are specifically concerned with the protection of private data. By complying with this internationally recognized guide and independently reviewing it, AWS demonstrates its commitment to customer content privacy.

Further information on our sub-processors and their certifications can be found here: https://aws.amazon.com/compliance/gdpr-center/

HubSpot Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141

We use Hubspot as a CRM to keep records of customer interactions. Hubspot may process personal data also in the Unites States of America. (Privacy Shield certified).

Intercom R&D Unlimited Company, Stephen Court, 18-21 St. Stephen's Green, Dublin 2, Republic of Ireland,

We use Intercom for communicating with our customers qualifying as a processor for personal data if you provide personal data in conversations with our customer support specialists.

Nylas, Inc., 944 Market St., San Francisco, CA, 94102.

Service provider for the email and calendar sync features. (Privacy Shield certified).

Visma Solutions Oy, Aurakatu 8, 20100 Turku

Service provider user for processing accounting information. Data processes only in EU/EEA.