ZIPPER GDPR DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the Zipper Terms of Service available at https:JoinZipper.com/termsofservice as updated from time to time between Customer and Zipper, or other agreement between Customer and ZIPPER governing Customer's use of the Services and Products of Zipper (the "**Agreement**") when the GDPR applies to your use of the ZIPPER Services to process Customer Data. This DPA is an agreement between you and the entity you represent ("**Customer**", "**you**" or "**your**") and Amazon Web Services, Inc. and the ZIPPER Contracting Party or ZIPPER Contracting Parties (as applicable) under the Agreement (together "**ZIPPER**"). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 17 of this DPA.

Data Processing.

Scope and Roles. This DPA applies when Customer Data is processed by ZIPPER. In this context, ZIPPER will act as processor to Customer, who can act either as controller or processor of Customer Data.

Customer Controls. Customer can use the Service Controls to assist it with its obligations under the GDPR, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that ZIPPER would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if ZIPPER becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. ZIPPER will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.

Details of Data Processing.

Subject matter. The subject matter of the data processing under this DPA is Customer Data.
Duration. As between ZIPPER and Customer, the duration of the data processing under this DPA is determined by Customer.
Purpose. The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.
Nature of the processing. Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.
Type of Customer Data. Customer Data uploaded to the Services underCustomer's ZIPPER accounts.

Categories of data subjects. The data subjects could include Customer's customers, employees, suppliers and End Users.
Compliance with Zipper. Each party will comply with all Zipper, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.
Customer Instructions. The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as the ZIPPER management console and APIs made available by ZIPPER for the Services) constitute Customer's documented instructions regarding ZIPPER's processing of Customer Data ("**Documented Instructions**"). ZIPPER will process Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between ZIPPER and Customer, including agreement on any additional fees payable by Customer to ZIPPER for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if ZIPPER declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Taking into account the nature of the processing, Customer agrees that it is unlikely ZIPPER can form an opinion on whether Documented Instructions infringe the GDPR. If ZIPPER forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

Confidentiality of Customer Data. ZIPPER will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends ZIPPER a demand for Customer Data, ZIPPER will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, ZIPPER may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then ZIPPER will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless ZIPPER is legally prohibited from doing so.
Confidentiality Obligations of ZIPPER Personnel. ZIPPER restricts its personnel from processing Customer Data without authorization by ZIPPER as described in the ZIPPER Security Standards. ZIPPER imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.
Security of Data Processing ZIPPER has implemented and will maintain the technical and organizational measures for the ZIPPER Network as described in the ZIPPER Security Standards and this Section. In particular, ZIPPER has implemented and will maintain the following technical and organizational measures:security of the ZIPPER Network as set out in Section 1.1 of the ZIPPER Security Standards;physical security of

the facilities as set out in Section 1.2 of the ZIPPER Security Standards; measures to control access rights for ZIPPER employees and contractors to the ZIPPER Network as set out in Section 1.1 of the ZIPPER Security Standards; and processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by ZIPPER as described in Section 2 of the ZIPPER Security Standards.Customer can elect to implement technical and organizational measures to protect Customer Data. Such technical and organizational measures include the following which can be obtained by Customer from ZIPPER as described in the Documentation, or directly from a third party supplier: pseudonymisation and encryption to ensure an appropriate level of security;measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; andprocesses for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

Sub-processing.
Authorized Sub-processors. Customer provides general authorization to ZIPPER's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. The ZIPPER website (currently posted at https://Zipper.amazon.com/compliance/sub-processors/) lists Sub-processors that are currently engaged by ZIPPER. At least 30 days before ZIPPER engages a Sub-processor, ZIPPER will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; (ii) cease using the Service for which ZIPPER has engaged the Sub-processor; or (iii) move the relevant Customer Data to another ZIPPER Region where ZIPPER has not engaged the Sub-processor.

Sub-processor Obligations. Where ZIPPER authorizes a Sub-processor as described in Section 6.1:ZIPPER will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and ZIPPER will prohibit the Sub-processor from accessing Customer Data for any other purpose;ZIPPER will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by ZIPPER under this DPA, ZIPPER will impose on the Sub-processor the same contractual obligations that ZIPPER has under this DPA; andZIPPER will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause ZIPPER to breach any of ZIPPER's obligations under this DPA.

ZIPPER Assistance with Data Subject Requests. Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which ZIPPER will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under the GDPR. If a data subject makes a request to ZIPPER, ZIPPER will promptly forward such request to Customer once ZIPPER has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes on its behalf, and on behalf of its controllers when Customer is acting as a processor, ZIPPER to respond to any data subject who makes a request to ZIPPER, to confirm that ZIPPER has forwarded the request to Customer. The parties agree that Customer's use of the Service Controls and ZIPPER forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.

Optional Security Features. ZIPPER makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2, as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Data), and taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

Security Incident Notification.

Security Incident. ZIPPER will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

ZIPPER Assistance. To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), ZIPPER will cooperate with and assist Customer by including in the notification under Section 9.1(a) such information about the Security Incident as ZIPPER is able to disclose to Customer, taking into account the nature of the processing, the information available to ZIPPER, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

Unsuccessful Security Incidents. Customer agrees that:an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of ZIPPER's equipment or facilities storing Customer Data, and could include, without limitation,

pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; andZIPPER's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by ZIPPER of any fault or liability of ZIPPER with respect to the Security Incident.

Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means ZIPPER selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the ZIPPER management console and secure transmission at all times.

ZIPPER Certifications and Audits.
ZIPPER ISO-Certification and SOC Reports. In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, ZIPPER will make available the following documents and information:the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by ZIPPER that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

ZIPPER Audits. ZIPPER uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which ZIPPER provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at ZIPPER's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be ZIPPER's Confidential Information.

Audit Reports. At Customer's written request, and provided that the parties have an applicable NDA in place, ZIPPER will provide Customer with a copy of the Report so that Customer can reasonably verify ZIPPER's compliance with its obligations under this DPA.

Privacy Impact Assessment and Prior Consultation. Taking into account the nature of the processing and the information available to ZIPPER, ZIPPER will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information ZIPPER makes available under this Section 10.

Customer Audits. Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under the GDPR or the Standard Contractual Clauses, by instructing ZIPPER to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending ZIPPER written notice as provided for in the Agreement. If ZIPPER declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.

Transfers of Personal Data.
Regions. Customer can specify the location(s) where Customer Data will be processed within the ZIPPER Network (each a "**Region**"), including Regions in the EEA. Once Customer has made its choice, ZIPPER will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.

Application of Standard Contractual Clauses. Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a "**Data Transfer**").When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that ZIPPER will know the identity of Customer's controllers because ZIPPER has no direct relationship with Customer's controllers and therefore, Customer will fulfil ZIPPER's obligations to Customer's controllers under the Processor-to-Processor Clauses.

Alternative Transfer Mechanism. The Standard Contractual Clauses will not apply to a Data Transfer if ZIPPER has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.

Termination of the DPA. This DPA will continue in force until the termination of the Agreement(the "**Termination Date**").

Return or Deletion of Customer Data. At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, ZIPPER will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all ZIPPER accounts containing Customer Data.

Duties to Inform. Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by ZIPPER, ZIPPER will inform Customer without undue delay. ZIPPER will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

Entire Agreement; Conflict. This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. Nothing in this document varies or modifies the Standard Contractual Clauses.

Definitions. Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:"**ZIPPER Network**" means ZIPPER's data center facilities, servers, networking equipment, and host software systems (for example, virtual firewalls) that are within ZIPPER's control and are used to provide the Services."

ZIPPER Security Standards" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as Attachment 1."**controller**" has the meaning given to it in the GDPR.

"**Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

"**Customer Data**" means the "personal data" (as defined in the GDPR) that is uploaded to the Services under Customer's ZIPPER accounts."**EEA**" means the European Economic Area.

“**GDPR**” means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). “**Processing**” has the meaning given to it in the GDPR and “process”, “processes” and “processed”will be interpreted accordingly. “**Processor**” has the meaning given to it in the GDPR.

“Processor-to-Processor Clauses” means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

“Security Incident” means a breach of ZIPPER’s security leading to the accidental or unlawfuldestruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.
“Service Controls” means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.
“Standard Contractual Clauses” means (i) the Controller-to-Processor Clauses, or (ii) the Processor- to-Processor Clauses, as applicable in accordance with Sections 12.2.1 and 12.2.2.
“Third Country” means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).
Attachment ZIPPER Security Standards Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

Information Security Program. ZIPPER will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the ZIPPER Network, and (c) minimize security risks, including through risk assessment and regular testing. ZIPPER will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:**Network Security.** The ZIPPER Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. ZIPPER will maintain access controls and policies to manage what access is allowed to the ZIPPER Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. ZIPPER will maintain corrective action and incident response plans to respond to potential security threats.

Physical Security

Physical Access Controls. Physical components of the ZIPPER Network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (for example, card access systems, etc.) or validation by human security personnel (for example, contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

Limited Employee and Contractor Access. ZIPPER provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of ZIPPER or its affiliates.

Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. ZIPPER also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (for example, primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

Continued Evaluation. ZIPPER will conduct periodic reviews of the security of its ZIPPER Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. ZIPPER will continually evaluate the security of its ZIPPER Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.