Zapier, Inc.

Data Processing Addendum

Version: May 18, 2021

This Data Processing Addendum ("Addendum") forms part of the Zapier online Terms of Service or other written agreement entered into between Zapier, Inc. ("Zapier") and you that incorporates this Addendum by reference (the "Agreement"), and governs the Processing of Personal Information by Zapier, acting as a Data Processor or Service Provider, in providing its online technology service (the "Service") pursuant to the Agreement.

As this Addendum is incorporated into and forms a part of the Agreement, separate signatures are not required. However, if you would like to complete a countersigned copy of this Addendum for your records, you can follow the e-signature process available on the Zapier website.

1 Definitions

1.1 "Data Subject" means any individual about whom Personal Information may be Processed under this Addendum.

1.2 "Data Protection Legislation" means the GDPR (as defined below), together with any national implementing laws in any Member State of the European Union or the United Kingdom or, to the extent applicable, data privacy laws of any other country, state or province, including the California Consumer Privacy Act, in each case as amended, repealed, consolidated or replaced from time to time.

1.3 "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 with regard to the processing of personal data and on the free movement of such data.

1.4 "Personal Information" means personal data or personal information (as defined under the Data Protection Legislation) that are subject to the Data Protection Legislation and that you authorize Zapier to collect and process on your behalf in connection with Zapier's provision of the Service under the Agreement.

1.5 "Process" or "Processing" means any operation or set of operations performed on Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.6 "Processor" means a natural or legal person, public authority, agency or other body which processes Personal Information on behalf of the controller (as such term is defined under the applicable Data Protection Legislation).

1.7 "Security Incident" means a breach of security of the Service or Zapier's systems used to Process Personal Information leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information.

1.8 "Sensitive Information" means Personal Information revealing a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation.

1.9 "Service Provider" means an entity that performs services on behalf of a business pursuant to the

Agreement using Personal Information that the business provides it (as such term is defined under the applicable Data Protection Legislation).

2 Details of the Processing.

2.1 **Categories of Data Subjects.** Refer to Appendix 1 of the Model Contract (defined below).

2.2 **Types of Personal Information.** Refer to Appendix 1 of the Model Contract (defined below).

2.3 **Subject-Matter and Nature of the Processing.** The subject-matter of Processing of Personal Information by Zapier is the provision of the Services to you that involves the Processing of Personal Information. Personal Information will be subject to those Processing activities which Zapier needs to perform in order to provide the Services pursuant to the Agreement.

2.4 **Purpose of the Processing.** Personal Information will be Processed by Zapier for purposes of providing the Services set out into the Agreement.

2.5 **Duration of the Processing.** Personal Information will be Processed for the duration of the Agreement, subject to Section 12 of this Addendum.

3 Limitations on Use. Zapier will Process Personal Information solely as a Processor or Service Provider on your behalf and in accordance with the Agreement, this Addendum and any other documented instructions from you (whether in written or electronic form), which includes your configuration and use of the Service, or as otherwise required by applicable law. Notwithstanding anything to the contrary in the Agreement, Zapier shall not (1) retain or use Personal Information other than as provided for in the Agreement or in the Service, or as needed to perform the Service, or (2) sell or otherwise disclose such Personal Information except as needed to render the Service. Zapier is hereby instructed to Process Personal Information to the extent necessary to enable Zapier to provide the Service in accordance with the Agreement. In case Zapier cannot process Personal Information in accordance with your instructions due to a legal requirement under any applicable law to which Zapier is subject, Zapier shall (i) promptly notify you in writing (including by e-mail) of such legal requirement before carrying out the relevant Processing, to the extent permitted by the applicable law, and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Information) until such time as you provide Zapier with new instructions. You will be responsible for providing or making Personal Information available to Zapier in compliance with the Data Protection Legislation, including providing any necessary notices to, and obtaining any necessary consents from, Data Subjects whose Personal Information is provided by you to Zapier for Processing pursuant to this Addendum. You acknowledge that the Service is not intended or designed for the Processing of Sensitive Information, and you agree not to provide any Sensitive Information through the Service. The parties agree that you provide Personal Information to Zapier as a condition precedent to Zapier's performance of the Service and that Personal Information is not exchanged for monetary or other valuable consideration. You acknowledge that Zapier is an independent controller when carrying out any activities not related solely to Zapier's Processing of Personal Information added by you to the Service (such as Zapier's management of its online forum, customer accounts and marketing programme).

4 Security. Zapier shall implement, and maintain throughout the term of the Addendum at all times in accordance with then current good industry practice, appropriate technical and organizational measures to protect Personal Information in accordance with Article 32 of the GDPR. On request, Zapier shall provide you with a written description of the security measures being taken. The Service provides reasonable technical and organizational measures that have been designed, taking into account the nature of its Processing, to assist you in securing Personal Information Processed by Zapier. Zapier will also assist you with conducting any legally required data protection impact assessments (including subsequent consultation with a supervisory authority), if so required by the

Data Protection Legislation, taking into account the nature of Processing and the information available to Zapier. Zapier may charge a reasonable fee for any such assistance, as permitted by applicable law.

5 **Confidentiality.** Zapier will ensure that its personnel authorized to process Personal Information are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6 **Data Subject Requests.** You are responsible for handling any requests or complaints from Data Subjects with respect to their Personal Information Processed by Zapier under this Addendum. Zapier will notify you promptly and in any event within fifteen (15) business days' of receipt, unless prohibited by applicable law, if Zapier receives any such requests or complaints. The Service include technical and organizational measures that have been designed, taking into account the nature of its Processing, to assist customers, insofar as this is possible, in fulfilling their obligations to respond to such requests or complaints.

7 **Regulatory Investigations.** At your request, Zapier will assist you in the event of an investigation by a competent regulator, including a data protection regulator or similar authority, if and to the extent that such investigation relates to the Processing of Personal Information by Zapier on your behalf in accordance with this Addendum. Zapier may charge a reasonable fee for such requested assistance except where such investigation arises from a breach by Zapier of the Agreement or this Addendum, to the extent permitted by applicable law.

8 **Security Incident.** In the event that Zapier becomes aware of a Security Incident, Zapier will notify you promptly and in any event no later than forty-eight (48) hours after Zapier discovers the Security Incident. In the event of such a Security Incident, Zapier shall provide you with a detailed description of the Security Incident and the Personal Information concerned, unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. Zapier will take reasonable steps to mitigate the effects of the Security Incident and to minimize any damage resulting from the Security Incident. At your request, Zapier will provide reasonable assistance and cooperation with respect to any notifications that you are legally required to send to affected Data Subjects and regulators.

9 **Sub-Processors.** You agree that Zapier may disclose Personal Information to its subcontractors for purposes of providing the Service ("**Sub-Processors**"), provided that Zapier (i) shall enter into an agreement with its Sub-Processors which comply with Data Protection Legislation, including requiring the Sub-Processors to only process Personal Information to the extent required to perform the obligations sub-contracted to them, and (ii) shall remain liable for the obligations subcontracted to, and the acts and omissions of, the Sub-Processors. Zapier's current list of Sub-Processors is located on Zapier's Subprocessor webpage at https://www.zapier.com/help/gdpr. Zapier will inform you of any intended changes concerning the addition or replacement of Sub-Processors by updating its Sub-Processor webpage, which you acknowledge is your responsibility to check regularly. You can subscribe to receive notifications when any changes are made to Zapier's Sub-Processors by following the instructions on the Sub-Processor webpage. You may object to such changes on reasonable grounds of data protection within ten (10) business days after being notified of the engagement of the Sub-Processor. If you object to a new Sub-Processor, as permitted in the preceding sentence, Zapier will use reasonable efforts to make available to you a change in the Service or recommend a commercially reasonable change to your configuration or use of the Service to avoid Processing of Personal Information by the objected-to new Sub-Processor. If Zapier is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may terminate the component of the Service which cannot be provided by Zapier without the use of the objected-to new Sub-Processor by providing written notice to the other party. Zapier will refund you any prepaid fees covering the remainder of the term of your subscription following the effective date of termination with respect to such terminated component of the Service, without imposing a penalty for such termination on you.

10 **Data Transfers.** In connection with the performance of the Agreement, you authorize Zapier to transfer Personal Information internationally, and in particular to locations outside of the United Kingdom and European Economic Area, such as the United States. If required to ensure Zapier's Processing of Personal Information complies with any international transfer rules set out in Data Protection Legislation, you and Zapier hereby enter into the Standard Contractual Clauses for the Transfer of Personal Information to Processors Established In Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010 Countries ("**Model Contract**"), incorporated into this Addendum by reference, as if it had been set out in full and completed at Exhibit A. Any replacement to the Model Contract adopted in accordance with Article 93(2) of the GDPR shall supersede the Model Contract incorporated into this Addendum automatically, and Exhibit A to this Addendum shall be interpreted instead so as to give full effect to such replacement Model Contract.

11 **Information.** Zapier shall make available to you all information necessary to demonstrate compliance with the obligations laid down in this Addendum and allow for and contribute to audits, including inspections, conducted by you or an auditor mandated by you. Zapier shall immediately inform you if, in its opinion, an instruction infringes the Data Protection Legislation.

12 **Return or Disposal.** Promptly following termination of your User Account for any reason, Zapier will destroy the Personal Information it was Processing on your behalf pursuant to Zapier's provision of the Service.

The parties' authorized signatories have duly executed this Addendum:

Zapier:

Suk Kim

Name: Suk Kim
General Counsel

You:

By:

Your Legal Name:

Name of Signatory:

Title of Signatory (if applicable):

Date:

Exhibit A – Processing Details

This Exhibit completes the template/blank sections of the Model Contract, which are incorporated into this Exhibit as if they had been set out in full. This Exhibit only applies if it is required to ensure Zapier's Processing of Personal Information on your behalf complies with Data Protection Legislation:

Model Contract: main body particulars:

Exporter contact details	Zapier's contact details as set out in the Agreement.
Importer contact details	Your contact details as set out in the Agreement.
Governing Law (cl. 9 & 11)	The law of the country in which the data exporter's EU representative or data subject is established/ based (as appropriate).

Appendix 1 of the Model Contract:

Data Exporter	You.
Data Importer	Zapier (a provider of a web-based, application integration and data linking service which Processes Personal Information upon instruction of the data exporter in accordance with the Agreement).
Data Subjects	Data exporter may submit Personal Information to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Information relating to the following categories of data subjects: *Data exporter's employees, contractors, representatives, agents, and other individuals whom data exporter permits to use the Service, as well as Personal Information relating to the data exporter's customers, partners, users and vendors.*
Categories of data	Data exporter may submit Personal Information to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following Personal Information: *First and Last Name, Billing Address, Phone number, IP Address, API Key, Access Token, User Identifiers, Password, Integration Configuration, API Logs, Cookies*
Special categories of data	None and the data exporter is prohibited from using the Service to process any such data under the terms of the Agreement.
Processing operations	The performance of the Service pursuant to the Agreement.
Appendix 2 of the Model Contract: **Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c)**	As set out in Exhibit B and supplemented by Exhibit C.

The illustrative indemnity set out in the Model Contract Clauses is deemed deleted.

Exhibit B – Technical and Organisational Measures

Zapier will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Information uploaded to the Service, as described in this Exhibit B. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the DPA.

A. SECURITY GOVERNANCE

Zapier maintains an information security program (including the adoption and enforcement of internal policies and procedures) designed to: (a) help our customers secure their data processed using Zapier's online product against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the Zapier online product, and (c) minimise security risks, including through risk assessment and regular testing. Zapier's head of security coordinates and is primarily responsible for the company's information security program.

The team covers the following core functions:

- Application security (secure development, security feature design, the Security Champions program, and secure development training)
- Infrastructure security (data centers, cloud security, and strong authentication)
- Monitoring and incident response (cloud native and custom)
- Vulnerability management (vulnerability scanning and resolution)
- Compliance and technical privacy
- Security awareness (onboarding training and awareness campaigns)

B. ACCESS CONTROL

i) Preventing Unauthorized Product Access

Third party data hosting and processing: We host our Service with third party cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. Their physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: Customers who interact with the products via the user interface are required to authenticate before they are able to access their non-public data. We support two-factor authentication and highly recommend that each customer enable two-factor authentication on their Zapier account. Zapier also supports Single-Sign On for Team and Company accounts.

Authorization: User Content (data originated by customers that a customer transmits through Zapier online service) is stored in multi-tenant storage systems which are only accessible to Customers via application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our 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. Authorization credentials are stored encrypted.

ii) Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support our 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.

Static code analysis: Automated security reviews of code stored in our source code repositories, performed through static code analysis, checking for coding best practices and identifiable software vulnerabilities.

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

Red teaming: Zapier performs annual offensive security exercises that target our internal corporate and production infrastructure and applications. The event is conducted in the form of a Red Team where highly qualified offensive operators are collaborating with our Security Operations Center. The exercise concludes with a remediation and validation phase where findings are addressed and the fixes validated.

Bug bounty: A bug bounty program invites and incentivizes independent security researchers to ethically discover and disclose security flaws. We implement a bug bounty program in an effort to widen the available opportunities to engage with the security community and improve the product defenses against sophisticated attacks.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our personnel have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of personnel is to provide effective customer support, troubleshoot potential problems, detect and respond to security incidents, and implement data security.

Personnel Security: Zapier personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Zapier conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local law and regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Zapier's confidentiality and security policies. Personnel are provided with security training.

C. ENCRYPTION TECHNOLOGIES

In-transit: We make HTTPS encryption (also referred to as SSL or TLS) available on all of our login interfaces and for free on every customer site hosted on the Zapier products. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

D. INPUT CONTROLS

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

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, and/or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and customer damage or unauthorized disclosure. Notifications will be in accordance with the terms of the Agreement.

E. DATA DELETION AND PORTABILITY

Zapier enables customers to delete their account and delete or export their account data in a manner consistent with the functionality of the Zapier product. Instructions and related details are provided within the applicable functionality within the Zapier product.

F. AVAILABILITY CONTROLS

Our 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 our operations in maintaining and updating the product applications and backend while limiting downtime.

Redundancy: The infrastructure providers use designs to eliminate single points of failure and minimize the impact of anticipated environmental risks. Zapier's product is designed to allow the company to perform certain types of preventative and corrective maintenance without interruption.

Business Continuity: Zapier has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

Exhibit C – Supplementary Measures adopted to address the European Data Protection Board's Recommendations

Challenges to information requests

1.1 In the event Zapier receives an order from any government authority for compelled disclosure of Personal Information relating to your customers as part of Zapier's provision of the Service under the Agreement, Zapier shall:

1.1.1 use every reasonable effort to redirect the government authority to request data directly from you;

1.1.2 promptly notify you of the request, unless prohibited under the law applicable to the requesting government authority or Zapier (and, if prohibited from notifying you, use reasonable lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to you) as soon as possible; and

1.1.3 use reasonable lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable Member State law.

1.2 For purposes of paragraph 1.1 of this Exhibit, lawful efforts means exercising the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a provider engaged in a similar type of undertaking under the same or similar circumstances and shall not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

Notification of Orders

1.3 Zapier shall provide reasonable cooperation to you in order for you to inform Data Subjects about any legally binding order for disclosure of their Personal Information by a government authority, unless:

1.3.1 providing such information proves impossible or unreasonable;

1.3.2 it can be reasonably expected that the Data Subject already has the information; or

1.3.3 such disclosure is otherwise legally prohibited (and in such case, paragraph 1.1 of this Exhibit above shall apply).

Transparency Reporting

1.4 Zapier shall inform you about access orders received from government authorities concerning Personal Information Processed under this Agreement relating to your customers, such information to consist at least of the number of orders, the nature of data demanded, the legal basis for such orders, and the identity of the ordering bodies, unless such information proves impossible for Zapier to provide, or the disclosure of such information is otherwise legally prohibited.

1.5 If the disclosure contemplated at paragraph 1.4 of this Exhibit is legally prohibited, then paragraph 1.1 of this Exhibit shall apply. Zapier shall distinguish between cases where copies of Personal Information is and is not requested. In its law enforcement transparency reporting, it shall provide additional details on the types of responses where it legally can do so, such as by providing information on the number of US demands versus demands from other countries.

Notification of Material Changes in applicable law

1.6 Zapier shall regularly review, assess and continuously monitor the scope of disclosures of Personal Information related to your customers in response to the orders of law enforcement and other government authorities it receives, as well as the safeguards and recourse in place to protect Data Subjects, and inform you promptly if it becomes aware of a change in applicable law that would materially impact such access by authorities or recourse available to Data Subjects.

Duty to Cooperate

1.7 Upon reasonable request, Zapier shall provide you with all information, documentation, and reasonable assistance as required to enable you to comply with the requirements for the transfer of personal data to Zapier pursuant to Chapter V of the GDPR (including any mandatory requirements by competent regulators or the European Data Protection Board and relevant court decisions) taking into account the specific tasks and responsibilities of Zapier as a Processor in the context of the Processing to be carried out and the risk to the rights and freedoms of the Data Subjects pursuant to the Agreement.