# Zapier Data Processing Addendum

*Last Updated: March 9, 2023*

This Data Processing Addendum ("**Addendum**") forms part of the Terms of Service or Enterprise 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 in providing its automation platform (the "**Service**") pursuant to the Agreement.

1. Definitions

1.1. "**Adequacy Decision**" means:

a. for data processed subject to the GDPR: the EEA, or a country or territory that is the subject of an adequacy decision issued by the European Commission under Article 45(1) of the GDPR; and

b. for data processed subject to the UK GDPR: the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018.

1.2. "**CCPA**" means Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (the California Consumer Privacy Act).

1.3. "**Controller to Processor SCCs**" means the Module Two (transfer controller to processor) of the European Commission Implementing Decision (EU) 2021/914, which can be found here: https://www.zapier.com/legal/standard-contractual-clauses, as updated or replaced from time to time.

1.4. "**CPA"** means Colo. Rev. Stat. §§ 6-1-1301 et seq. (the Colorado Privacy Act).

1.5. "**CTDPA**" means Connecticut's Data Privacy Act.

1.6. "**Data Subject**" means any individual whose Personal Information may be Processed under this Addendum.

1.7. "**Data Protection Legislation**" means applicable law governing the use, access to, deletion of, or Processing of Personal Information under this Addendum, including, but not limited to, the CCPA, the CPA, the CTDPA, the UCPA, the VCDPA, the GDPR, and UK GDPR, together with any national or subordinate legislation and regulations implementing,in each case as amended, repealed, consolidated, or replaced from time to time.

1.8. "**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.

1.9. "**Personal Information**" means personal data or personal information (as defined under the applicable Data Protection Legislation) that is 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.

1.10. "**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.

1.11. "**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 GDPR).

1.12. "**Processor to Processor SCCs**" means the Module Three (transfer processor to processor) of the European Commission Implementing Decision (EU) 2021/914, which can be found here: https://www.zapier.com/legal/standard-contractual-clauses, as updated and/or replaced from time to time.

1.13. "**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 Processed by Zapier. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Information, including unsuccessful login attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems

1.14. "**Sensitive Information**" means the types of sensitive Personal Information set forth in Article 9, Section 1 of the GDPR.

1.15. "**Service Provider**" means an entity that receives Personal Information and is prohibited from retaining, using, selling, or disclosing such information other than in connection with providing the Service pursuant to the Agreement.

1.16. "**Subprocessor List**" means Zapier's Subprocessors as identified on https://www.zapier.com/legal/subprocessors.

1.17. "**Swiss Amendments**" mean the Controller to Processor SCCs or the Processor to Processor SCCs (as applicable) with the following amendments: (a) "FDPIC" means the Swiss Federal Data Protection and Information Commissioner, (b) "Revised FADP" means the revised version of the FADP of 25 September 2020, which is scheduled to come into force on 1 January 2023, (c) the term "EU Member State" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their

rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c), (d) the Controller to Processor SCCs also protect the data of legal entities until the entry into force of the Revised FADP, and (e) the FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP.

1.18. "**UCPA**" means Utah Code Ann. §§ 13-61-101 et seq. (the Utah Consumer Privacy Act).

1.19. "**UK Addendum**" means the template Addendum B.1.0 issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, and in force from 21 March 2022, available here: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf as updated and/or replaced from time to time. For the purposes of the UK Addendum, (a) the information required for Table 1 is contained in Schedule 1 of this Addendum, and the start date shall be the commencement of the Service, (b) in relation to Table 2, the version of the EU Clauses to which the UK Approved Addendum applies is Module Two for Controller to Processor where Zapier is acting as your Processor and Module Three for Processor to Processor where Zapier is acting as your Subprocessor, (c) in relation to Table 3, the list of parties and description of the transfer are as set out in Schedule 1 of this Addendum, Zapier's technical and organizational measures are set out in Schedule 1 of this Addendum, and the list of Zapier's Subprocessors is as provided in Section 8 of this Addendum, and (d) in relation to Table 4, neither party will be entitled to terminate the UK Addendum in accordance with clause 19 of Part 2 of the UK Addendum.

1.20. "**UK GDPR**" means the GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

1.21. "**U.S. Privacy Laws**" collectively mean the CCPA, the CPA, the CTDPA, the UCPA, and the VCDPA.

1.22. "**VCDPA**" means VA Code Ann. §§ 59.1-575 et seq. (the Virginia Consumer Data Protection Act).

2. Details of the Processing

2.1. **Categories of Data Subjects.** As set out in Schedule 1.

2.2. **Types of Personal Information.** As set out in Schedule 1.

2.3. **Subject-Matter and Nature of the Processing.** The subject-matter of Processing of Personal Information by Zapier is the provision of the Service 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 Service pursuant to the Agreement.

2.4. **Purpose of the Processing.** Personal Information will be Processed by Zapier for purposes of providing the Service 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 11 of this Addendum.

3. Processing Requirements.

3.1. 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), or as otherwise required by applicable law.

3.2. Notwithstanding anything to the contrary in the Agreement, Zapier shall not (a) retain, use or disclose Personal Information other than as provided for in the Agreement or as needed to perform the Service, (b) "sell" (as such term is defined by U.S. Privacy Laws), "share," (as such term is defined by the CCPA). Zapier is hereby instructed to Process Personal Information to the extent necessary to enable Zapier to provide the Service in accordance with the Agreement and this Addendum, or (c) Process Personal Information except as necessary for the business purposes specified in the Agreement or this Addendum.

3.3. 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 (a) 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 (b) cease all Processing (other than merely storing and maintaining the security of the affected Personal Information) until you provide Zapier with new instructions.

3.4. You will be responsible for providing or making Personal Information available to Zapier in compliance with all applicable Data Protection Legislation, including providing any necessary notices to, and obtaining and maintaining any necessary rights, consents, and authortizations from, Data Subjects whose Personal Information is provided by you to Zapier for Processing pursuant to this Addendum. Each of Zapier and you acknowledge and agree that you have not "sold" (as such term is defined by the CCPA) Personal Information to Zapier.

3.5. You acknowledge and agree that you, rather than Zapier, are responsible for certain configurations and design decisions for the Service and that you, and not Zapier, are responsible for implementing those configurations and design decisions in a secure manner that complies with applicable Data Protection Legislation. Without limiting the foregoing, you represent, warrant, and covenant that you shall only transfer Personal Information to Zapier using secure, reasonable, and appropriate mechanisms.

3.6. 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.

3.7. 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, analytics, customer accounts, and marketing program).

4. Security. Zapier shall implement and maintain throughout the term of the Addendum reasonable and appropriate technical and organizational measures designed to protect Personal Information against unauthorized or accidental access, loss, alteration, disclosure, or destruction, including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, and encryption. Zapier will also provide reasonable assistance to you with conducting any legally required data protection impact assessments with respect to the Processing of Personal Information by Zapier (including, where necessary, subsequent consultation with a supervisory authority with jurisdiction over such Processing), if so required by the Data Protection Legislation, taking into account the nature of Processing and the information available to Zapier.

5. Security Incident. If Zapier becomes aware of a Security Incident, Zapier will (a) notify you without undue delay, and not later than 48 hours after Zapier discovers the Security Incident, and (b) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects, and remediate the cause to the extent within Zapier's reasonable control. Upon your request and taking into account the nature of the applicable Processing, Zapier will assist by providing, when available, information reasonably necessary for you to meet your Security Incident notification obligations under Data Protection Laws. You acknowledge that Zapier providing notification of a Security Incident is not an acknowledgment of fault or liability.

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

7. 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. If Zapier receives a request from your Data Subject in relation to the Data Subject's Personal Information Processed under your Service account, Zapier will notify you and advise the Data Subject to submit the request to you, and you will be responsible for responding to any such request.

8. Subprocessors. In providing the Service, you agree that:

8.1. Zapier engages the organizations listed on the Subprocessor List (each a "**Subprocessor**") to help Process Personal Information on the Service.

8.2. Zapier will enter into a written agreement with each Subprocessor imposing data processing and protection obligations substantially the same as those set out in this Addendum.

8.3. Zapier will maintain a current list of its Subprocessors, including their functions and locations, as specified in the Subprocessor List.

8.4. Zapier may update the Subprocessor List from time to time. In the event that Zapier seeks to add any Subprocessors and update the Subprocessor List, Zapier will provide notice of such additions to you (which may be via email, a posting, or notification on an online portal for our services, or other reasonable means).

8.5. In the event that you do not wish to consent to the use of such additional Subprocessor, you may notify Zapier that you do not consent within fifteen (15) days based on reasonable data protection concerns. In such case, the parties will discuss such concerns in good faith.

8.6. If the parties are unable to reach a mutually agreeable resolution to your objection to a new Subprocessor, you, as your sole and exclusive remedy, may terminate the Order for the affected Service for convenience, and Zapier will refund any prepaid, unused fees for the terminated portion of the applicable Term.

9. 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 Personal Information is Processed in a country that has not received an Adequacy Decision, you and Zapier hereby enter into:

9.1. the **Controller to Processor SCCs** if the restricted transfer is subject to the GDPR and Zapier is acting as your Processor;

9.2. the **Processor to Processor SCCs** if the restricted transfer is subject to the GDPR and Zapier is acting as your Subprocessor;

9.3. the **Swiss Amendments** if the restricted transfer consists of Personal Information originating from Switzerland; and

9.4. the **UK Addendum** if the restricted transfer is subject to the UK GDPR.

10. Information.

10.1. Zapier shall make available its privacy and security policies and other such information necessary to demonstrate compliance with the obligations set forth in this Addendum.

10.2. Upon reasonable notice and appropriate confidentiality agreements, and taking into account the nature of the applicable Processing, Zapier will assist

you in fulfilling your obligations under applicable Data Protection Laws to carry out a data protection impact or similar risk assessment related to your use of the Service, including, if required by Data Protection Laws, by assisting you in consultations with relevant government authorities.

11. Return or Disposal. Promptly following termination of the Agreement and this Addendum for any reason, Zapier will destroy the Personal Information it was Processing on your behalf pursuant to Zapier's provision of the Service unless Data Protection Legislation prevents Zapier from destroying all or part of the Personal Information.

12. Modification. Notwithstanding anything to the contrary in the Agreement, Zapier may periodically modify this Addendum as required to comply with Data Protection Legislation.

**The parties' authorized signatories have duly executed this Addendum:**

**Zapier:**

Suk Kim

**Name:** Suk Kim
General Counsel

**You:**

**By:** Ole Nepomuk Mai

**Your Legal Name:** Ole Nepomuk Mai

**Name of Signatory:** Ole Nepomuk Mai

**Title of Signatory (if applicable):** Owner (Inhaber)

**Date:** 06 / 24 / 2023

## Schedule 1

## LIST OF PARTIES

**Data exporter(s):**

| | |
|---|---|
| **Name** | You |
| **Address** | As detailed in the communications between us from time to time. |
| **Contact person's name, position, and contact details** | As detailed in the communications between us from time to time. |
| **Activities relevant to the data transferred under these Clauses** | Receipt of the Service |
| **Role (controller/processor)** | Controller or Processor |

**Data importer(s):**

| | |
|---|---|
| **Name** | Zapier |
| **Address** | As listed above. |
| **Contact person's name, position, and contact details** | Suk Kim, General Counsel<br>privacy@zapier.com |
| **Activities relevant to the data transferred under these Clauses** | Provision of the Service |
| **Role (controller/processor)** | Processor |

**DESCRIPTION OF TRANSFER**

| |
|---|
| **Categories of data subjects whose personal data is transferred**<br>**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:**<br><br>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 personal data transferred**

**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, Credit Card Information, IP Address, API Key, Access Token, User Identifiers, Password, Integration Configuration, API Logs, Cookies

**Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

None, and the data exporter is prohibited from using the Service to process any such data under the terms of the Agreement.

**The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).**

Continuous basis

**Nature of the processing**

The performance of the Service pursuant to the Agreement.

**Purpose(s) of the data transfer and further processing**

The performance of the Service pursuant to the Agreement.

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

For the duration of the Agreement.

**For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**

Located on Zapier's Subprocessor webpage at https://www.zapier.com/legal/subprocessors.

**TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

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

1. Security Governance

1.1. 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 unauthorized access to the Zapier online product, and (c) minimize 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.

1.2. The team covers the following core functions:

a. Application security (secure development, security feature design, the Security Champions program, and secure development training)

b. Infrastructure security (data centers, cloud security, and strong authentication)

c. Monitoring and incident response (cloud native and custom)

d. Vulnerability management (vulnerability scanning and resolution)

e. Compliance and technical privacy

f. Security awareness (onboarding training and awareness campaigns)

2. Access Control

2.1. **Preventing Unauthorized Product Access**

a. *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 the Addendum. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

b. *Physical and environmental security***:** We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls of such providers

are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

c. *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.

d. *Authorization*: Customer 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.

e. *Application Programming Interface (API) access*: Public product APIs may be accessed using an API key or through OAuth authorization. Authorization credentials are stored encrypted.

2.2. **Preventing Unauthorized Product Use.** We implement industry-standard access controls and detection capabilities for the internal networks that support our products.

a. *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.

b. *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.

c. *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.

d. *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.

e. *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.

2.3. **Limitations of Privilege & Authorization Requirements**

a. *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.

b. *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.

c. 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.

3. Encryption Technologies

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

3.2. **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.

4. Input Controls

4.1. **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.

4.2. **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.

5. 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.

6. 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.

6.1. **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.

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

Dropbox Sign

# Audit trail

| | |
|---|---|
| **Title** | Zapier DPA |
| **File name** | Data Processing A...(2023-03-09).docx |
| **Document ID** | b9ad7cd81cc9d29ee8ca8f0447ba7f333a517d50 |
| **Audit trail date format** | MM / DD / YYYY |
| **Status** | Signed |

## Document history

| | | |
|---|---|---|
| SENT | **06 / 24 / 2023**<br>21:10:55 UTC | Sent for signature to Ole Nepomuk Mai (info@olemai.de) from accounting@zapier.com<br>IP: 3.84.212.110 |
| VIEWED | **06 / 24 / 2023**<br>21:11:08 UTC | Viewed by Ole Nepomuk Mai (info@olemai.de)<br>IP: 84.173.3.40 |
| SIGNED | **06 / 24 / 2023**<br>21:12:45 UTC | Signed by Ole Nepomuk Mai (info@olemai.de)<br>IP: 84.173.3.40 |
| COMPLETED | **06 / 24 / 2023**<br>21:12:45 UTC | The document has been completed. |