Note: Below is a reference copy of Zapier's previous Data Processing Addendum from April 1, 2026. Please note that this agreement is now outdated; it was replaced by Zapier's current Data Processing Addendum, which may be accessed at: https://www.zapier.com/legal/data-processing-addendum.

Data Processing Addendum

Because Zapier's Terms of Service already incorporate Zapier's Data Processing Addendum ("**DPA**"), you do not need to sign a separate copy. This DPA (and the accompanying Standard Contractual Clauses) contain legal terms that apply to personal information that may be contained in Customer Content. We've updated the DPA as of April 1, 2026, to be effective as of April 7, 2026.

If you need a standalone copy of Zapier's DPA for your records or other compliance purposes, you can generate an electronically signed copy of the DPA. You will receive two emails from Zapier Dropbox Sign (noreply@mail.hellosign.com):

> The first will be a request to sign with the subject: "Zapier DPA - Signature requested by Zapier Dropbox Sign."
>
> Once you sign and agree to the DPA terms, you will receive a second email with the subject: "You just signed" that contains a fully signed PDF copy of the DPA.
>
> If you have any trouble receiving these messages, check your spam folder, wait at least five minutes for each email to arrive, and ensure you clicked the final "Agree" button after signing in Dropbox Sign.

***

Zapier Data Processing Addendum

Last Updated: April 1, 2026

Effective: April 7, 2026

Previous version

This Data Processing Addendum ("**DPA**") forms part of the Terms of Service or Enterprise Agreement (in either case, the "**Agreement**") entered into between Zapier, Inc. ("**Zapier**") and you that incorporates this DPA by reference. This DPA governs the processing of Personal Information by Zapier in providing the Service (as defined in the Agreement). This DPA does not apply to

Personal Information once transferred from the Service to a Third-Party Service (as defined in the Agreement), as your agreement with that Third-Party Service will instead govern.

1. Definitions

1.1. "**Applicable Data Protection Law**" means applicable law governing the use of, access to, deletion of, or processing of Personal Information under this DPA, including, but not limited to, U.S. Data Protection Laws and European Data Protection Laws, together with any national or subordinate legislation and regulations implementing, in each case as amended, repealed, consolidated, or replaced from time to time.

1.2. "**Brazilian Data**" means Personal Information that is subject to the protection of the Lei Geral de Proteção de Dados ("**LGPD**").

1.3. "**commercial purpose**", "**controller**", "**processor**", "**data subject**", "**processing**" (and "**process**"), "**service provider**", and "**supervisory authority**" each have the meaning given to them in Applicable Data Protection Law, as appropriate.

1.4. "**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.

1.5. "**Data Privacy Framework**" means the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework, and the UK Extension to the EU-US Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce, as may be amended, superseded, or replaced from time to time.

1.6. "**Data Privacy Framework Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as may be amended, superseded, or replaced from time to time.

1.7. "**Europe**" means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.

1.8. "**European Data**" means Personal Information that is subject to the protection of European Data Protection Laws.

1.9. "**European Data Protection Laws**" mean (a) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Information and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (b) in respect of the United Kingdom, the Data Protection Act 2018 and the EU GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and (c) the Swiss Federal Data Protection Act and its

implementing regulations ("**Swiss FADP**"); in each case as may be amended, superseded or replaced from time to time.

1.10. "**Personal Information**" means (a) personal data or personal information (as defined under the Applicable Data Protection Law) that is subject to the Applicable Data Protection Law and (b) that is contained within Customer Content, for which you authorize Zapier to collect and process on your behalf in connection with Zapier's provision of the Service under the Agreement.

1.11. "**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.

1.12. "**Security Incident**" means a confirmed 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.

1.13. "**Sensitive Information**" means any Personal Information (a) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (b) that is genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation; (c) relating to criminal convictions and offenses; and (d) any other form of Personal Information that is afforded enhanced protection under the Applicable Data Protection Law.

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

1.15. "**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.

1.16. "**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 of the UK Addendum is contained in Schedule 1 of this DPA, and the start date shall be the commencement of the Service; (b) in relation to Table 2 of the UK Addendum, 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 of the UK Addendum, the list of parties and description of the transfer are as set out in Schedule 1 of this DPA, Zapier's technical and organizational measures are set out in Schedule 2 of this DPA, and the list of Zapier's Subprocessors is as provided in Section 9 of this DPA; and (d) in relation to Table 4 of the UK Addendum, neither party will be entitled to terminate the UK Addendum in accordance with clause 19 of Part 2 of the UK Addendum.

1.17. "**U.S. Data Protection Laws**" mean all state laws in effect in the United States of America that are applicable to the processing of Personal Information under this DPA, including, but not limited to, the California Consumer Privacy Act, as amended by the California Privacy Rights act ("**CCPA**"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

2. Description of 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 Processing.** The subject matter of processing of Personal Information by Zapier is the provision of the Service to you that involves processing of Personal Information. Personal Information will be subject to those processing activities that 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 in 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 DPA.

3. Processing Requirements

3.1. Zapier will process Personal Information in its capacity as processor (a) for the purpose of providing and supporting the Service in accordance with the Agreement, this DPA, and any other documented lawful instructions from you (whether in written or electronic form); (b) to develop, enhance, and improve the Service as provided by the Agreement; and (c) as otherwise required by applicable law. Zapier will at all times comply with U.S. Data Protection Laws and European Data Protection Laws in processing Personal Information under the Agreement.

3.2. Notwithstanding anything to the contrary in the Agreement, consistent with Applicable Data Protection Law, 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 CCPA) or “share,” (as such term is defined by CCPA)**;** (c) process Personal Information except as necessary for the business purposes specified in the Agreement or this DPA; or (d) retain, use, disclose, or otherwise process Personal Information outside of the direct business relationship with Customer and not combine Personal Information with personal information that it receives from other sources, except as permitted under the CCPA. Further, Zapier shall notify Customer if it makes a determination that it can no longer meet its obligations under CCPA or CPRA.

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 are solely responsible for (a) the accuracy, quality, and legality of Personal Information and the means by which you acquired Personal Information; (b) complying with all necessary transparency and lawfulness requirements under Applicable Data Protection Law for the collection and use of Personal Information, including obtaining any necessary consents and authorizations; (c) ensuring you have the right to transfer, or provide access to, Personal Information to Zapier for processing in accordance with the terms of the Agreement (including this DPA); and (d) ensuring that your instructions to Zapier regarding the processing of Personal Information comply with applicable laws, including Applicable Data Protection Law.

3.5. You are responsible for independently determining whether the data security provided for in the Service adequately meets your obligations under Applicable Data Protection Law. You acknowledge and agree that you are solely responsible for (a) certain configurations and design decisions for the Service and (b) for implementing those configurations and design decisions in a secure manner that complies with Applicable Data Protection Law. 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 Agreement reasonable and appropriate technical and organizational measures designed to protect Personal Information against unauthorized or accidental access, loss, alteration, disclosure, or destruction, as further described in Schedule 2 of this DPA (Technical and Organizational Measures). 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 Applicable Data Protection Law, 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 the Applicable 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 DPA. 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. You may access, delete, and export Personal Information in accordance with the processes described at https://zapier.com/legal/data-retention-deletion.

8. Audits.

8.1. To the extent necessary and required by Applicable Data Protection Law, you may, at your sole expense, conduct a reasonable audit pursuant to a mutually agreed-upon audit plan with Zapier that is consistent with the requirements of this Section 8.

8.2. You may exercise such audit right: (a) to the extent Zapier's provision of third-party audit reports (e.g., Service Organization Control (SOC) 2 reports) do not provide sufficient information to verify Zapier's compliance with this DPA; and (b) where required by Applicable Data Protection Law or a relevant government authority.

8.3. Each such audit must: (a) be conducted by you or through a third-party auditor on your behalf that will enter into a confidentiality agreement with Zapier; (b) be limited in scope to matters reasonably required to assess Zapier's compliance with this DPA and Applicable Data Protection Law; (c) occur no more than once annually (unless required under Applicable Data Protection Law); (d) cover only processing facilities directly controlled by Zapier; (e) restrict findings to your Personal Information only; and (f) treat any results as confidential information to the fullest extent permitted by Applicable Data Protection Law.

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

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

9.2. Zapier will enter into an agreement with each Subprocessor imposing data processing and protection obligations substantially the same as those set out in this DPA.

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

9.4. Zapier may update the Subprocessor List from time to time. In the event that Zapier updates the Subprocessor List, Zapier will provide fourteen (14) days' advance written notice (which may be via email, a posting, notification on an online portal for our services, or other reasonable means).

9.5. 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 fourteen(14) days of Zapier's advance written notice based on reasonable data protection concerns. In such case, the parties will discuss such concerns in good faith.

9.6. 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 subscription term for the affected Service.

10. Data Transfers.

10.1. In connection with the performance of the Agreement, you authorize Zapier to transfer Personal Information internationally, and in particular, that Personal Information may be transferred to and processed by Zapier in the United States and other jurisdictions where Zapier and its

Subprocessors have operations. Whenever Personal Information is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws.

10.2. To the extent applicable to you, you acknowledge that in connection with the performance of the Service, Zapier is a recipient of European Data and Brazilian Data in the United States. To the extent that Zapier receives European Data or Brazilian Data in the United States, Zapier will comply with the following:

10.2.1. *Data Privacy Framework*. Zapier will use the Data Privacy Framework to lawfully receive European Data in the United States, ensure that it provides at least the same level of protection to such European Data as is required by the Data Privacy Framework Principles, and let you know if Zapier is unable to comply with this requirement.

10.2.2. *Standard Contractual Clauses*. If the Data Privacy Framework is invalidated and/or does not cover the transfer of European or Brazilian Data to Zapier, the applicable standard contractual clauses will be incorporated by reference and form a part of this DPA as follows:

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

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

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

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

10.2.2.5. the **Standard Contractual Clauses set forth in Resolution CD/ANPD No. 19/2024** if the restricted transfer is subject to the LGPD.

11. Information.

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

11.2. 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 Applicable Data Protection Laws, by assisting you in consultations with relevant government authorities.

11.3. If a law enforcement agency sends Zapier a demand for Personal Information (e.g., a subpoena or court order), Zapier will attempt to redirect the law enforcement agency to request that data directly from you. As part of this effort, Zapier may provide your contact information to the law

enforcement agency. If compelled to disclose Personal Information to a law enforcement agency, then Zapier will give you reasonable notice of the demand to allow you to seek a protective order or other appropriate remedy, to the extent Zapier is legally permitted to do so.

12. Disposal. Promptly following termination of the Agreement and this DPA for any reason, Zapier will destroy the Personal Information it was processing on your behalf pursuant to Zapier's provision of the Service unless Applicable Data Protection Law prevents Zapier from destroying all or part of the Personal Information.

13. Modification. Notwithstanding anything to the contrary in the Agreement, Zapier may periodically modify this DPA as required to comply with Applicable Data Protection Law.

Schedule 1

LIST OF PARTIES

Data exporter(s):

Name	You
Address	As provided in the "Notices" section of the Agreement.
Contact person's name, position, and contact details	As provided in the "Notices" section of the Agreement.
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	548 Market St. #62411 San Francisco, CA 94104-5401 United States
Contact person's name, position, and contact details	Suk Kim, General Counsel 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 **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 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, contact information such as address and email address, IP address, user identifier.

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.

Schedule 2

TECHNICAL AND ORGANIZATIONAL MEASURES

For the generally released Service that is not a Beta Release, Zapier will maintain administrative, physical, and technical safeguards, as described in Sections 1 to 6 below. All capitalized terms

not otherwise defined herein shall have the meanings as set forth in the DPA.

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 products against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to Zapier products, 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

b. Infrastructure security

c. Monitoring and incident response

d. Vulnerability management

e. Governance, risk, and compliance

f. Security awareness

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 DPA. We rely on contractual and data protection agreements, 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 certain higher-tier 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 by 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 product infrastructure. The technical measures implemented differ between infrastructure providers and may 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.

d. *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 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 on every customer site hosted on 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 potentially 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 accounts and delete or export their account data in a manner consistent with the functionality of Zapier products. Instructions and related details are provided within the applicable functionality of Zapier products.

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 of preventing single points of failure. This design assists our operations in maintaining and updating 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 products are 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.

7. Beta Releases. For Beta Releases (as defined in the Agreement), only this Section 7 shall apply. For Beta Releases, Zapier will maintain 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.