Zapier, Inc.

Data Processing Addendum

This Data Processing Addendum ("Addendum") forms part of the Terms of Service, Developer Platform Agreement 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 in providing its task automation service (the "Service") pursuant to the Agreement.

If you would like to complete a countersigned copy of this Addendum for your records, the following are the instructions for completing such a copy:

1. This Addendum consists of two parts: the main body of the Addendum, and its Schedules (including all Annexes and Exhibits thereof).

2. This Addendum has been pre-signed on behalf of Zapier. The Standard Contractual Clauses in the Schedules have been pre-signed by Zapier as the data importer.

3. To complete a countersigned copy of this Addendum, you must:

    - Complete the information in the signature box and sign this Addendum below.
    - Send the completed and signed Addendum to Zapier by email to contact@zapier.com.

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or, to the extent applicable, in any other country, and the California Consumer Privacy Act, in each case as amended, repealed, consolidated or replaced from time to time.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 GDPR).

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 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.

2 Details of the Processing.

2.1 **Categories of Data Subjects.** Refer to Annex 1 of the Appendix of the 2021 Model Contract (defined below) set out in Schedule 1.

2.2 **Types of Personal Information.** Refer to Annex 1 of the Appendix of the 2021 Model Contract (defined below) 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 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 11 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), 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 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, analytics, 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. 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 as described in Annex II of the 2021 Model Clauses attached to this Addendum. 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 if we can identify that the request is a Data Subject included in your data set, 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 you, insofar as this is possible, in fulfilling your 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 seventy-two (72) 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. Zapier may charge a reasonable fee for such requested assistance.

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 fully liable for all obligations subcontracted to, and all acts and omissions of, the Sub-Processors. Zapier's current list of Sub-Processors (or a hyperlink to such list) is located at: https://zapier.com/help/account/data-management/data-privacy-at-zapier. 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 Data 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: (i) the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries pursuant to Module 2 of the European Commission Implementing Decision (EU) 2021/914 ("**2021 Model Contract**"), which is incorporated into this Addendum in full and completed at Schedule 1; or (ii) the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established In Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010 (which is incorporated into Schedule 2 as if they had been set out in full) ("**2010 Model Contract**") if you are based in the United Kingdom. Any replacement or modifications to the 2010 Model Contract and/or the 2021 Model Contract adopted in accordance with Article 93(2) of the GDPR or recommended by the relevant territory's Supervisory Authority shall supersede the relevant 2010/2021 Model Contract incorporated into the Schedules automatically, and the relevant Schedule shall be interpreted instead so as to give full effect to such replacement Model Contract.

11 **Return or Disposal.** Promptly following termination of your User Account for any reason, Zapier will delete the Personal Information it was Processing on your behalf pursuant to Zapier's provision of the Service. Additionally, Zapier will delete the Personal Information Zapier is Processing on your behalf in accordance with the data retention periods described in https://zapier.com/help/account/data-management/data-privacy-at-zapier.

The parties' authorized signatories have duly executed this Addendum:

Zapier:

You:

REFERENCE COPY – DO NOT EXECUTE
To initiate an electronically signed copy, visit: https://zapier.com/help/account/data-management/zapiers-data-processing-addendum or https://zapier.com/help/account/data-management/data-privacy-at-zapier

By:

Name:

Your Legal Name:

Name of Signatory:

Title of Signatory (if applicable):

Date:

Schedule 1
Controller to Processor 2021 Standard Contractual Clauses (Module 2)

SECTION I

Clause 1

1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6;

(ii) Clause 8 (Module Two): Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 (Module Two): Clause 9(a), (c), (d) and (e);

(iv) Clause 12 (Module Two): Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 (Module Two): Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the

redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. The Parties agree that at the end of the provision of the Processing services the Importer shall delete all Personal Data and shall certify to the Exporter that it has done so. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

The parties acknowledge that the Importer complies with its obligations under this clause 8.9 in connection with its sub-processors by exercising its contractual audit rights it has agreed with such sub-processors.

Clause 9

9 Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to

the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

10 Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

12 Liability

(a) Each Party shall be liable to the other Party for any damages it causes the other Party by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party that part of the compensation corresponding to its responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

13 Supervision

(a) If the data exporter:

(i) is established in the EU, the competent supervisory authority shall be the Irish Data Protection Commissioner;

(ii) is not established in an EU Member State, and has appointed a representative pursuant to Article 27(1) regulation (EU) 2016/679, it shall notify the data importer of this and the EU Member State in which the exporter's representative is appointed shall be the competent supervisory authority; and

(iii) is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) but has not appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: the data exporter shall notify the data importer of its chosen competent supervisory authority, which must be the supervisory authority of a Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

14 Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority

to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

15 Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination,

make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

For the purposes of Clause 14(c), 15.1(b) and 15.2, the Parties agree that "best efforts" and the obligations of the data importer under clause 15.2 shall mean exercising the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a leading practice 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.

SECTION IV – FINAL PROVISIONS

Clause 16

16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

17 Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

18 Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I to 2021 Standard Contractual Clauses

A. 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 Services
Role (controller/processor)	Controller

Data importer(s):

Name	Zapier
Address	As listed above.
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 Services
Role (controller/processor)	Processor

B. 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, 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 List located (or hyperlink to list available) at: https://zapier.com/help/account/data-management/data-privacy-at-zapier.

ANNEX II to 2021 Standard Contractual Clauses

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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 Annex II. 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.

ANNEX III to 2021 Standard Contractual Clauses

LIST OF SUB-PROCESSORS

Zapier's current list of Sub-Processors (or a hyperlink to such list) is located at: https://zapier.com/help/account/data-management/data-privacy-at-zapier.

Schedule 2
2010 Standard Contractual Clauses (only applicable to UK residents)
Exhibit A – Processing Details

This Exhibit completes the template/blank sections of the 2010 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:

2010 Model Contract: main body particulars:

Exporter contact details	Your contact details as set out in the Agreement.
Importer contact details	Zapier's 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 2010 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, Credit Card Information, 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 2010 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 Annex II of Schedule 1 and supplemented by Exhibit B of this Schedule 2.

Exhibit B – 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 third party for compelled disclosure of Personal Data 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 third party to request data directly from you;

1.1.2 promptly notify you of the request, unless prohibited under the law applicable to the requesting third party (and, if prohibited from notifying you, use all 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 Data by an 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 authorities concerning Personal Data 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 Data 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 Data related to your customers in response to the orders of law enforcement and other 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.