# DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is subject to and forms part of your Stripe Services Agreement and governs Stripe's and its Affiliates' Processing of Personal Data.

1. **Structure.** If your Stripe Account is located in North America or South America, you enter this DPA with Stripe, Inc. ("**SINC**"). If your Stripe Account is located elsewhere, you enter this DPA with Stripe Payments Europe, Limited ("**SPEL**"). Accordingly, references in this DPA to "**Stripe**" mean SINC or SPEL, as applicable. If your Stripe Services Agreement is with an SSA Affiliate, Stripe may engage that SSA Affiliate to Process Personal Data according to this DPA.

2. **Definitions.** Capitalized terms not defined in this DPA have the meanings given to them in your Stripe Services Agreement.

   "**Approved Data Transfer Mechanism**" means, as applicable, the EEA SCCs, the UK Data Transfer Addendum or any data transfer mechanism a supervisory authority approves under DP Law that is incorporated into this DPA.

   "**Authorized Services**" means Services that a Governmental Authority licenses, authorizes or regulates.

   "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code Sections 1798.100-1798.199.

   "**DP Law**" means all Law that applies to Personal Data Processing under your Stripe Services Agreement and this DPA, including international, federal, state, provincial and local Law relating to privacy, data protection or data security.

   "**Data Controller**" means the entity which, alone or jointly with others, determines the purposes and means of Processing Personal Data, which may include, as applicable, a "Business" as defined under the CCPA.

   "**Data Processor**" means the entity that Processes Personal Data on behalf of the Data Controller, which may include, as applicable, a "Service Provider" as defined under the CCPA.

   "**Data Security Measures**" means technical and organizational measures that are intended to secure Personal Data to a level of security appropriate for the risk of the Processing.

   "**Data Subject**" means an identified or identifiable natural person to which Personal Data relates.

   "**EEA**" means the European Economic Area.

   "**EEA SCCs**" mean Module 2 (Transfer: Controller to Processor) of the standard contractual clauses set out in the European Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries according to the GDPR.

   "**GDPR**" means the General Data Protection Regulation (EU) 2016/679.

   "**Instructions**" means this DPA and any further written agreement or documentation under which the Data Controller instructs a Data Processor to perform specific Processing of Personal Data for that Data Controller.

   "**Joint Controller**" means a Data Controller that jointly determines the purposes and means of Processing Personal Data with one or more Data Controllers.

   "**Personal Data**" means any information relating to an identified or identifiable natural person that is Processed in connection with the Services, and includes "personal data" as defined under the GDPR and "personal information" as defined under the CCPA.

"**Process**" means to perform any operation or set of operations on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying, as described under DP Law.

"**Sensitive Data**" means (a) Personal Data that is genetic data, biometric data, data concerning health, a natural person's sex life or sexual orientation; or (b) data about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, to the extent this data is treated distinctly as a special category of Personal Data under DP Law.

"**SSA Affiliate**" means an Affiliate of Stripe that acts as (a) a Joint Controller with Stripe in relation to Authorized Services; or (b) a Data Processor on behalf of Stripe in relation to Services other than Authorized Services.

"**Sub-processor**" means an entity a Data Processor engages to Process Personal Data on that Data Processor's behalf in connection with the Services.

"**UK Data Transfer Addendum**" means the international data transfer addendum to the EEA SCCs issued by the United Kingdom's Information Commissioner's Office.

"**UK GDPR**" means the GDPR, as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

**3. Stripe as Data Processor and Data Controller.**

3.1. Data Processing Roles. To the extent Stripe Processes Personal Data as a:

(a) Data Processor, it is acting as a Data Processor on behalf of you, the Data Controller; and

(b) Data Controller, it has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through you.

3.2. Categories of Data Subjects and Personal Data.

(a) *Data Subjects.* Stripe may Process the Personal Data of your Customers, representatives and any natural persons who access or use your Stripe Account.

(b) *Personal Data.* Where applicable, Stripe may Process Payment Account Details, bank account details, billing/shipping address, name, date/time/amount of transaction, device ID, email address, IP address/location, order ID, payment card details, tax ID/status, unique customer identifier, identity information including government issued documents (e.g., national IDs, driver's licenses and passports).

(c) *Sensitive Data.* Where applicable, Stripe may Process facial recognition data.

3.3. Data Processing Purposes**.**

(a) The purposes of Stripe's Processing of Personal Data are when Stripe is operating in its capacity as a Data Processor for a Service, including:

(i) servicing the Stripe platform; and

(ii) facilitating payment transactions on behalf of Stripe users.

(b) The purposes of Stripe's Processing of Personal Data in its capacity as a Data Controller are:

(i) determining the Processing of Personal Data when providing Stripe products and services, including when Stripe provides a payment method, and determining the third parties (banks and payment method providers) to be utilized;

(ii) monitoring, preventing and detecting fraudulent transactions and other fraudulent activity on the Stripe platform;

(iii) complying with Law, including applicable anti-money laundering screening and know-your-customer obligations; and

(iv) analyzing and developing Stripe's services.

**4. Stripe Obligations when Acting as a Data Processor.**

4.1. Obligations. To the extent that Stripe is acting as a Data Processor for you, Stripe will:

(a) Process Personal Data on behalf of and according to your Instructions. Stripe will not sell, retain, use or disclose Personal Data for any purpose other than for the specific purposes of performing the Services and to comply with Law, unless otherwise permitted by your Stripe Services Agreement (including this DPA) or DP Law. Stripe will inform you if, in its opinion, Instructions violate or infringe DP Law;

(b) ensure that all persons Stripe authorizes to Process Personal Data in the context of the Services are granted access to Personal Data on a need-to-know basis and are committed to respecting the confidentiality of Personal Data;

(c) to the extent required by DP Law, inform you of requests Stripe receives from Data Subjects (including "verifiable consumer requests" as defined under the CCPA) exercising their applicable rights under DP Law to (i) access (e.g., right to know under the CCPA) their Personal Data; (ii) have their Personal Data corrected or erased; (iii) restrict or object to Stripe's Processing; or (iv) data portability. Other than to request further information, identify the Data Subject, and, if applicable, direct the Data Subject to you as Data Controller, Stripe will not respond to these requests unless you instruct Stripe in writing to do so;

(d) to the extent required by DP Law, inform you of each law enforcement request Stripe receives from a Governmental Authority requiring Stripe to disclose Personal Data or participate in an investigation involving Personal Data;

(e) to the extent required by DP Law, provide you with reasonable assistance through appropriate technical and organizational measures, at your expense, to assist you in complying with your obligations under DP Law, which assistance may include conducting data protection impact assessments and consulting with a supervisory authority, taking into account the nature of the Processing and the information available to Stripe;

(f) implement and maintain a written information security program with the Data Security Measures stated in Exhibit 1 of this DPA. In addition, Stripe will implement a data security incident management program that addresses how Stripe will manage a data security incident involving the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to, Personal Data ("**Incident**"). If Stripe is required by DP Law to notify you of an Incident, then Stripe will notify you without unreasonable delay, but in no event later than any time period required by DP Law. In

addition, for Incidents affecting Personal Data subject to GDPR or UK GDPR, Stripe will notify you no later than 48 hours after Stripe becomes aware of the Incident. Stripe will partner with you to respond to the Incident. The response may include identifying key partners, investigating the Incident, providing regular updates, and discussing notice obligations. Except as required by DP Law, Stripe will not notify your affected Data Subjects about an Incident without first consulting you;

(g) engage Sub-processors as necessary to perform the Services on the basis of the general written authorization you give to Stripe under Section 4.2 of this DPA;

(h) to the extent required by DP Law and upon your written request, contribute to audits or inspections by making audit reports available to you, which reports are Stripe's confidential information. Upon your written request, and no more frequently than once annually, Stripe will promptly provide documentation or complete a written data security questionnaire of reasonable scope and duration regarding Stripe's and its Affiliates' Processing of Personal Data. All documentation provided, including any response to a security questionnaire, is Stripe's confidential information; and

(i) at your choice, and subject to Stripe's rights and obligations under your Stripe Services Agreement (including this DPA), delete or return all Personal Data to you after the Term, and delete existing copies held by Stripe, unless Stripe is required or authorized by DP Law to store Personal Data for a longer period.

4.2 Sub-processors.

(a) You specifically authorize Stripe to engage its Sub-processors and Affiliates from the agreed lists of Sub-processors and Affiliates at stripe.com/service-providers/legal ("**Stripe Service Providers List**"). If you subscribe to email notifications at the Stripe Service Providers List, then Stripe will notify you via email of any changes Stripe intends to make to the Stripe Service Providers List at least 30 days before the changes take effect. You may reasonably object to a change on legitimate grounds within 30 days after you receive notice of the change. You acknowledge that Stripe's Sub-processors are essential to provide the Services and that if you object to Stripe's use of a Sub-processor, then notwithstanding anything to the contrary in your Stripe Services Agreement (including this DPA), Stripe will not be obligated to provide you the Services for which Stripe uses that Sub-processor.

(b) Stripe will enter into a written agreement with each Sub-processor that imposes on that Sub-processor obligations comparable to those imposed on Stripe under this DPA, including implementing appropriate Data Security Measures. If a Sub-processor fails to fulfill its data protection obligations under that agreement, Stripe will remain liable to you for the acts and omissions of its Sub-processor to the same extent Stripe would be liable if performing the relevant Services directly under this DPA.

4.3 CCPA Certification. To the extent applicable to the Services, Stripe certifies that it understands and will comply with the requirements in this DPA relating to the CCPA.

4.4 **Disclaimer of Liability. Notwithstanding anything to the contrary in your Stripe Services Agreement or this DPA, Stripe and its Affiliates will not be liable for any claim made by a Data Subject arising from or related to Stripe's or any of its Affiliates' acts or omissions, to the extent that Stripe was acting in accordance with your Instructions.**

**5. Your obligations when acting as a Data Controller.** You must:

5.1 only provide Instructions to Stripe that are lawful;

5.2 comply with and perform your obligations under DP Law, including with regard to Data Subject rights, data security and confidentiality, and ensure you have an appropriate legal

basis for the Processing of Personal Data as described in your Stripe Services Agreement, including this DPA; and

5.3 provide Data Subjects with all necessary information (including by means of offering a transparent and easily accessible public privacy notice) regarding, respectively, Stripe's and your Processing of Personal Data for the purposes described in your Stripe Services Agreement, including this DPA.

**6. Data transfers.**

6.1 General. Stripe and its Affiliates may transfer Personal Data on a global basis as necessary to provide the Services. In particular, Stripe and its Affiliates may transfer Personal Data to SINC in the United States and to Stripe's Affiliates and Sub-processors in other jurisdictions. Where Stripe transfers Personal Data under this DPA to a country or recipient not recognised as having an adequate level of protection for Personal Data according to DP Law, Stripe will comply with its obligations under DP Law.

6.2 Transfers from the EEA to SINC. The EEA SCCs apply to a transfer from the EEA of Personal Data Processed under this DPA between you and SINC and are incorporated into this DPA. You agree that the EEA SCCs are completed and supplemented as follows:

(a) you are the data exporter and SINC is the data importer;
(b) the optional docking clause under Clause 7 of the EEA SCCs will not apply;
(c) option 2 under Clause 9 of the EEA SCCs applies and you generally authorize SINC to engage Sub-processors according to Section 4.2 of this DPA;
(d) the optional redress language under Clause 11(a) of the EEA SCCs will not apply;
(e) the governing law under Clause 17 of the EEA SCCs will be Ireland;
(f) the choice of forum and jurisdiction under Clause 18 of the EEA SCCs will be the courts of Ireland;
(g) Annexes I, II and III of the EEA SCCs are deemed to be populated with the information set out in Exhibits 1 and 2 of this DPA; and
(h) Annex IV of Exhibit 2 of this DPA supplements the EEA SCCs with additional clauses.

6.3 2010 SCCs. For the purposes of a transfer of Personal Data from the EEA, Switzerland or the United Kingdom, any reference to the standard contractual clauses adopted under Directive 95/46/EC ("**2010 SCCs**") in an agreement you have entered into with Stripe or its Affiliates will be construed as a reference to the Approved Data Transfer Mechanism. The 2010 SCCs are terminated and replaced by the Approved Data Transfer Mechanism. Any Personal Data transferred under the 2010 SCCs will not be returned or destroyed due to the termination of the 2010 SCCs and instead will become subject to the Approved Data Transfer Mechanism.

6.4 Transfers from the United Kingdom to SINC. The UK Data Transfer Addendum applies to a transfer from the United Kingdom of Personal Data Processed under this DPA between you and SINC and is incorporated into this DPA. You agree that the UK Data Transfer Addendum is completed and supplemented as follows:

(a) you are the data exporter and SINC is the data importer;
(b) Table 1 of the UK Data Transfer Addendum is deemed to be populated with the information set out in Annex IA of Exhibit 2 of this DPA;
(c) for the purposes of Table 2 of the UK Data Transfer Addendum, the version of the "Approved EU SCCs" (including the appendix information, modules and selected clauses) appended to the UK Data Transfer Addendum is the EEA SCCs:
(d) the optional docking clause under Clause 7 of the EEA SCCs will not apply;
(e) option 2 under Clause 9 of the EEA SCCs applies and you generally authorize SINC to engage Sub-processors according to Section 4.2 of this DPA;
(f) the optional redress language under Clause 11(a) of the EEA SCCs will not apply;

(g) Annex IV of Exhibit 2 of this DPA supplements the EEA SCCs with additional clauses;
(h) Table 3 of the UK Data Transfer Addendum is deemed to be populated with the information set out in Exhibits 1 and 2 of this DPA;
(i) the "importer" and "exporter" option applies for the purposes of Table 4 of the UK Data Transfer Addendum;
(j) under Part 2, the mandatory clauses of the UK Data Transfer Addendum will apply; and
(k) by using the Services to transfer Personal Data to SINC, you will be deemed to have signed the UK Data Transfer Addendum.

6.5 Transfers from other countries or regions. The terms applicable to the transfer of Personal Data processed under this DPA from any country or territory listed in Exhibit 3 of this DPA, including any Approved Data Transfer Mechanism, are incorporated into this DPA.

**7. Conflict.** If there is any conflict or ambiguity between:

7.1 the provisions of this DPA and the provisions of your Stripe Services Agreement regarding Personal Data Processing, the provisions of this DPA will prevail; and

7.2 the provisions of this DPA and any provision contained in an Approved Data Transfer Mechanism and executed by you and SINC, the provisions of the Approved Data Transfer Mechanism will prevail.

# EXHIBIT 1: STRIPE DATA SECURITY

| | |
|---|---|
| **Security Programs and Policies** | Stripe maintains and enforces a security program that addresses how Stripe manages security, including the security controls Stripe employs. The security program includes:<br>● documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually;<br>● documented, clear assignment of responsibility and authority for security program activities;<br>● policies covering, as applicable, acceptable computer use, data classification, cryptographic controls, access control, removable media and remote access; and<br>● regular testing of the key controls, systems and procedures.<br>**Privacy Program.** Stripe maintains and enforces a privacy program and related policies that address how Personal Data is collected, used and shared. |
| **Risk and Asset Management** | Stripe performs risk assessments, and implements and maintains controls for risk identification, analysis, monitoring, reporting and corrective action.<br>Stripe maintains and enforces an asset management program that appropriately classifies and controls hardware and software assets throughout their life cycle. |
| **Personnel Education and Controls** | All (a) Stripe employees; and (b) Stripe independent contractors who may have access to data, including those who Process Personal Data ((a) and (b), collectively "**Personnel**") acknowledge their data security and privacy responsibilities under Stripe's policies.<br>For Personnel, Stripe, either itself or through a third party:<br>● implements pre-employment background checks and screening;<br>● conducts security and privacy training;<br>● implements disciplinary processes for violations of data security or privacy requirements; and<br>● upon termination or applicable role change, promptly removes or updates Worker access rights and requires the Worker to return or destroy Personal Data.<br>**Authentication**. Stripe authenticates each Personnel's identity through appropriate authentication credentials such as strong passwords, token devices or biometrics. |
| **Training and Awareness** | **Annual Security and Privacy Training.** Stripe's employees complete an annual Security and Privacy awareness training on Stripe's data security and confidentiality policies and practices. |
| **Network and Operations Management** | **Policies and Procedures**. Stripe implements policies and procedures for network and operations management. These policies and procedures address hardening, change control, segregation of duties, separation of development and production environments, technical architecture management, network security, malware protection, protection of data in transit and at rest, data integrity, encryption, audit logs and network segregation. |

| | |
|---|---|
| | **Vulnerability Assessments.** Stripe performs periodic vulnerability assessments and penetration testing on its systems and applications, including those that Process Personal Data. |
| **Technical Access Controls** | **Access control.** Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including the following measures:<br>● user identification and authentication procedures;<br>● ID/password security procedures (special characters, minimum length, change of password), including stronger digital authentication measures based on NIST 800-63B;<br>● automatic blocking (e.g., password or timeout); and<br>● break-in-attempt monitoring.<br>**Data access control.** Stripe implements measures to ensure that persons entitled to use a data processing system gain access only to the Personal Data allowed for their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including:<br>● internal policies and procedures;<br>● control authorization schemes;<br>● differentiated access rights (profiles, roles, actions and objects);<br>● access monitoring and logging;<br>● access reports;<br>● access procedure;<br>● change procedure; and<br>● deletion procedure. |
| **Physical access controls** | Stripe uses reputable third-party service providers to host its production infrastructure. Stripe relies on these third parties to manage the physical access controls to the data center facilities that they manage. Some of the measures that Stripe's service providers provide to prevent unauthorized persons from gaining physical access to the data processing systems available at premises and facilities (including databases, application servers and related hardware), where Personal Data is Processed, include:<br>● physical access control system and program in place at Stripe premises;<br>● 24x7 Global Security Operation Center that monitors physical security systems;<br>● security video and alarm systems;<br>● access control roles and area zones;<br>● access control audit measures;<br>● electronic tracking and management program for keys;<br>● access authorisations process for employees and third parties;<br>● door locking (electrified locks etc.); and<br>● trained uniformed security staff.<br>Stripe reviews third-party audit reports to verify that Stripe's service providers maintain appropriate physical access controls for the managed data centers. |

| | |
|---|---|
| **Availability Controls** | Stripe implements measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, including:<br>● database replication;<br>● backup procedures;<br>● hardware redundancy; and<br>● a disaster recovery plan. |
| **Disclosure Controls** | Stripe implements measures to ensure that Personal Data (a) cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic); and (b) can be verified to which companies or other legal entities Personal Data are disclosed, including logging, transport security and encryption. |
| **Entry Controls** | Stripe implements measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, including logging and reporting systems, and audit trails and documentation. |
| **Separation Controls** | Stripe implements measures to ensure that Personal Data collected for different purposes can be Processed separately, including:<br>● "least privilege" limitation of access to data by internal service;<br>● segregation of functions (production/testing);<br>● procedures for storage, amendment, deletion, transmission of data for different purposes; and<br>● logical segmentation processes to manage the separation of Personal Data. |
| **Certifications and Reports** | **PCI Compliance**. To the extent applicable to the Services, Stripe will provide the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by the PCI-DSS requirements. Stripe's certification is confirmed annually by a qualified security assessor (QSA).<br>**SOC Reports**. Stripe maintains Service Organization Controls ("**SOC**") auditing standards for service organizations issued under the AICPA. SOC 1 and 2 reports are produced annually and will be provided upon request.<br>Stripe may add standards or certifications at any time. |
| **Encryption** | Stripe applies data encryption mechanisms at multiple points in Stripe's service to mitigate the risk of unauthorized access to Stripe data at rest and in transit. Access to Stripe cryptographic key materials is restricted to a limited number of authorized Stripe personnel.<br>**Encryption in transit.** To protect data in transit, Stripe requires all inbound and outbound data connections to be encrypted using the TLS 1.2 protocol. For data traversing Stripe's internal production networks, Stripe uses mTLS to encrypt connections between production systems. |

| | |
|---|---|
| | **Encryption at rest.** To protect data at rest, Stripe uses industry standard encryption (AES 256) to encrypt all production data stored in server infrastructure.<br><br>**Payment Card and Banking Account Data Tokenization.** Payment card and bank numbers are separately encrypted using industry standard encryption (AES-256) at the data level and stored in a separate data vault that is highly restricted. Decryption keys are stored on separate machines. Tokens are generated to support Stripe data processing. |
| **Data Security Incident Management and Notification** | Stripe implements a data security incident management program that addresses how Stripe manages Incidents.<br><br>Stripe will notify impacted Stripe users and Governmental Authorities (where applicable) of Incidents in a timely manner as required by DP Law. |
| **Reviews, Audit Reports and Security Questionnaires** | Upon written request, and no more frequently than annually, Stripe will complete a written data security questionnaire of reasonable scope and duration regarding Stripe's business practices and data technology environment in relation to the Processing of Personal Data. Stripe's responses to the security questionnaire are Stripe's confidential data. |
| **System Configuration** | Stripe implements measures for ensuring system configuration, including default configuration measures for internal IT and IT security governance.<br><br>Stripe relies on deployment automation tools to deploy infrastructure and system configuration. These automation tools leverage infrastructure configurations that are managed through code that flows through Stripe's change control processes. Stripe's change management processes require formal code reviews and two-party approvals prior to the release to production.<br><br>Stripe uses monitoring tools to monitor production infrastructure for changes from known configuration baselines. |
| **Data Portability** | The Stripe API enables Stripe users to programmatically access the data stored for transfer, excluding PCI-scoped data. The portability process for PCI data to other PCI-DSS Level 1 compliant payment processors can be found at https://stripe.com/docs/security/data-migrations/exports. |
| **Data Retention and Deletion** | Stripe implements and maintains data retention policies and procedures related to Personal Data and reviews these policies and procedures as appropriate. |

# EXHIBIT 2: APPROVED DATA TRANSFER MECHANISM: DESCRIPTION OF PROCESSING AND TRANSFER

## ANNEX I

### A. LIST OF PARTIES

**Data exporter(s):**

**Name**: The party to the Stripe Services Agreement with Stripe or its Affiliate (as applicable).

**Address**: The data exporter's address.

**Contact person's name, position and contact details**: The name, position and contact details provided by the data exporter.

**Activities relevant to the data transferred under these Clauses:** Processing Personal Data in connection with the data exporter's use of the Services under the Stripe Services Agreement.

**Role (controller/processor):** Controller

**Signature and date:** By using the Services to transfer Personal Data to the data importer, the data exporter will be deemed to have signed this Annex I.

**Data importer:**

**Name**: Stripe, Inc.

**Registered office**: Corporation Trust Center, 1209 Orange Street, Wilmington, New Castle, DE 19801, USA

**Contact details:** Stripe Privacy Team, privacy@stripe.com

**Activities relevant to the data transferred under these Clauses:** Processing Personal Data in connection with the data exporter's use of the Services under the Stripe Services Agreement.

**Role (controller/processor):** Processor

**Signature and date:** The data importer will be deemed to have signed this Annex I on the transfer of Personal Data by the data exporter in connection with the Services.

### B. DESCRIPTION OF TRANSFER

***Categories of data subjects whose personal data is transferred***

The Personal Data transferred concern the following categories of Data Subjects or consumers:

- Users of the data importer's online and mobile services.

- The data exporter's end customers, donors, representatives and any natural person who accesses or uses your Stripe Account.

***Categories of personal data transferred***

The categories of Personal Data transferred are described in Section 3 of the DPA.

***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.***

The categories of Personal Data transferred are described in Section 3 of the DPA.

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

The frequency of the transfer is a continuous basis for the duration of the Stripe Services Agreement until the Personal Data is deleted in accordance with Section 4.1(i) of the DPA.

***Nature of the processing***

The nature of the processing is described in Section 3 of the DPA.

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

The purposes of the data transfer are described in Section 3 of the DPA.

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

The period for which the personal data will be retained is set out in Section 4.1(i) of the DPA.

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

The subject matter and nature of the processing related to transfers to Sub-processors is set out at Annex III to these clauses. Subject to Section 4.1(i) of the DPA, the duration of the processing is the duration of the Stripe Services Agreement.

**C. COMPETENT SUPERVISORY AUTHORITY**

The competent supervisory authority in accordance with Clause 13 of the EEA SCCs is the Irish Data Protection Commission.

## ANNEX II

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

The data importer will maintain and implement the technical and organizational measures set out in Exhibit 1 of the DPA.

## ANNEX III

LIST OF SUB-PROCESSORS

The controller has generally authorized the engagement of the Sub-processors at https://stripe.com/service-providers/legal.

## ANNEX IV

SUPPLEMENTAL CLAUSES

In addition to the obligations under the EEA SCCs and the UK Data Transfer Addendum (as applicable), the parties agree to the following supplementary measures:

1. Personal Data will be encrypted both in transit and at rest using encryption technology by the data importer.
2. the data importer will resist, to the extent permitted by Law, any request under Section 702 of Foreign Intelligence Surveillance Act ("**FISA**").
3. the data importer will use reasonably available legal mechanisms to challenge any demands for data access through the national security process that it may receive in relation to data exporter's data.
4. no later than the date on which the data exporter's acceptance of the DPA and the Approved Data Transfer Mechanism that incorporates or references this Annex becomes effective, the data importer will notify the data exporter of any binding legal demand for the Personal Data it has received, including national security orders and directives, which will encompass any process issued under Section 702 of FISA, unless prohibited under Law.
5. the data importer will ensure that Stripe's data protection officer has oversight of Stripe's approach to international data transfers.

This Annex also sets out the parties' interpretation of their respective obligations under the specific terms of the EEA SCCs (as amended or supplemented by an Approved Data Transfer Mechanism). Where a party complies with the interpretations set out in this Annex, that party will be deemed by the other party to have complied with its commitments under the EEA SCCs.

6. **Clause 8.1(a): Instructions**

   The DPA and the Stripe Services Agreement are the data exporter's complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately in writing by the parties. For the purposes of Clause 8.1(a) of the EEA SCCs, the Processing described in the DPA is deemed an instruction by the data exporter to Process Personal Data.

7. **Clause 9(c): Copies of Sub-processor Agreements**

   The parties agree that, following a request by the data exporter, the data importer will provide copies of the Sub-processor agreements that must be provided to the data exporter pursuant to Clause 9(c) of the EEA SCCs, provided that the data importer may (i) redact or remove all

commercial information, or clauses unrelated to the EEA SCCs or their equivalent and (ii) determine the manner in which to provide the copy agreements to the data exporter.

8. **Clause 8.9(k) and (l): Audit**

   The data exporter acknowledges and agrees that it exercises its audit right under Clause 8.9(k) and (l) of the EEA SCCs by instructing the data importer to comply with the audit measures described in Section 4.1(h) of the DPA.

9. **Additional commercial clause**

   The EEA SCCs are incorporated into the Stripe Services Agreement. As between the data exporter, and the data importer and its Affiliates, to the greatest extent permitted by Law, the limitations and exclusions of liability set out in the Stripe Services Agreement will apply to the EEA SCCs.

10. **Defined terms**

    Capitalized terms not defined in these Annexes have the meanings given to them in the Stripe Services Agreement, including the DPA.

# EXHIBIT 3: JURISDICTION SPECIFIC TERMS AND APPROVED DATA TRANSFER MECHANISMS

**SWITZERLAND**

The EEA SCCs in the form described in Section 6.2 of the DPA and as adapted and supplemented as described in this Exhibit 3, will only apply to a transfer of Personal Data Processed under this DPA from Switzerland to SINC. For these purposes, you agree that:

1. any reference to “Member State” will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland);

2. any references to “personal data” extend to personal data of legal entities if and to the extent such personal data pertaining to legal entities is within the scope of the Swiss Federal Act on Data Protection ("**FADP**"); and

3. to the extent the transfer of personal data is governed by the FADP, the Swiss Federal Data Protection and Information Commissioner will act as the competent supervisory authority; to the extent the transfer of personal data is governed by the GDPR, the supervisory authority determined in Annex IC will act as the competent supervisory authority; any references to the "competent supervisory authority" will be interpreted accordingly.