DATA PROCESSING AGREEMENT (DPA)

Stripe	Stripe Payments Europe, Ltd., a private limited company organized under the laws of Ireland ("**SPEL**")
User	Frappe Technologies Pvt Ltd, India
Effective Date	12/5/2021
Stripe Agreement	Stripe Services Agreement located at https://stripe.com/[country code]/legal, where "country code" means the two-letter abbreviation for the country where User is located

SIGNATURES	
Stripe Emma Redmond By: Emma Redmond	**User** DocuSigned by: Prakash Hodage 8AC40F6CA0A54E0... By: Prakash Hodage

SCOPE

This Data Processing Agreement ("**DPA**"), effective as of the Effective Date specified above, is between SPEL ("**Stripe**") and the user entity ("**User**") specified above and is subject to and incorporated into the Stripe Agreement.

Stripe and User agree as follows:

1. **Structure.** This DPA states the privacy, data protection and security requirements that apply to the Processing of Personal Data by Stripe and its Affiliates for the purpose of providing the Stripe Services to User under the Stripe Agreement. In addition, if Stripe or its Affiliates provide services to User or its Affiliates in any geographical region(s) outside the region covered by the Stripe Agreement, this DPA will apply and the corresponding Stripe services agreement will incorporate the terms of this DPA by reference.
2. **Definitions.** When used in this DPA, the following terms have the following meanings. Any capitalized terms not defined in this DPA have the meanings given to them in the Stripe Agreement.

   "**CCPA**" means the California Consumer Privacy Act of 2018, as may be amended or replaced from time to time.

   "**DP Law**" means all laws and regulations that apply to Personal Data Processing under the Stripe Agreement, including applicable international, federal, state, provincial, and local laws, rules, regulations, directives and governmental requirements currently in effect, and as they become effective, relating in any way to privacy, data protection or data security, and the Payment Card Industry ("**PCI**") Data Security Standards.

   "**Data Controller**" means the entity which, alone or jointly with others, determines the purposes and means to Process 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 appropriate for the risk of the Processing, which include measures protecting Personal Data from misuse, accidental or unlawful loss, and unauthorized access, disclosure, alteration, or destruction.

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

"**EEA Standard Contractual Clauses**" mean the standard contractual clauses set out in the European Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, as amended or replaced from time to time by a competent authority under the relevant DP Law.

"**GDPR"** means the General Data Protection Regulation (EU) 2016/679, as amended or replaced from time to time.

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

"**Personal Data**" means any information relating to a Data Subject (who can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person) that is collected, disclosed, stored, accessed or otherwise Processed under the Stripe Agreement.

"**Process**", "**Processing**" or "**Processed**" 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 defined or described under applicable DP Law.

"**Sensitive Data**" means Personal Data that is genetic data, biometric data, data concerning health, a natural person's sex life or sexual orientation; or 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 applicable DP Law.

"**Standard Contractual Clauses**" mean the EEA Standard Contractual Clauses and/or UK Standard Contractual Clauses, as applicable.

"**Sub-processor**" means an entity the Data Processor (or any Sub-processor of the Data Processor) engages to Process Personal Data on User's behalf in connection with the Stripe Agreement and this DPA.

"**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, as amended or replaced from time to time.

"**UK Standard Contractual Clauses**" mean the standard contractual clauses (processor) set out in Commission Decision 2010/87/EC and the standard contractual clauses (controller) set out in Commission Decision 2004/915/EC, as amended or replaced from time to time.

3. Stripe as Data Processor and Data Controller.

To the extent Stripe or its Affiliates Process Personal Data as a:

a. Data Processor (as described in the table below), it is acting as a Data Processor on behalf of User, the Data Controller; and

b. Data Controller (as described in the table below), it has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through User.

Data Processing concerns the following:	
Data Subjects	
User's customers and donors.	
Personal Data	
Includes where applicable: bank account details, billing/shipping address, card expiration date, customer or donor name, CVC code, 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 (including national IDs, driver's licenses and passports).	
Sensitive Data	
Where applicable, facial recognition data.	
Data Processing Purposes:	
Stripe as Data Processor	**Stripe as Data Controller**
• Servicing the Stripe platform; and • Facilitating payment transactions on behalf of Stripe users.	• Determining the processing of Personal Data when providing Stripe products and services to Stripe users, including determining the third parties (banks and payment method providers) to be utilized; • Monitoring, preventing and detecting fraudulent transactions and other fraudulent activity on the Stripe platform; • Determining the means and purposes of processing to comply with legal obligations or regulatory requirements that apply to the financial sector to which Stripe is subject, including applicable anti-money laundering screening and know-your-customer obligations; and • Analyzing and developing Stripe's products and services. Note: A Stripe Affiliate may act as Data Controller for activities which are licensed, authorised or regulated by a local regulatory authority.

4. Stripe Obligations when acting as a Data Processor.

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

a. Process Personal Data on behalf of and in accordance with User Instructions. Stripe will not sell, retain, use or disclose Personal Data for any purpose other than for the specific purposes of performing the Stripe Services and to comply with applicable Laws, unless otherwise permitted by the Stripe Agreement or DP Law. Stripe will inform User if, in its opinion, Instructions infringe DP Law;

b. ensure that all persons Stripe authorizes to Process Personal Data in the context of the Stripe 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 User of all formal requests Stripe receives from Data Subjects (including Verifiable Consumer Requests under CCPA) exercising their applicable

rights under DP Law to (i) access (right to know to 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. Stripe will not respond to these requests, unless User instructs Stripe in writing to do so;

d. to the extent required by DP Law, inform User of each request Stripe receives from a public authority requiring Stripe to disclose Personal Data Processed in the context of the Stripe Services or participate in an investigation involving that Personal Data;

e. to the extent required by DP Law, provide reasonable assistance through appropriate technical and organizational measures to User, at User's expense, to assist User in complying with User's obligations under DP Law, which assistance would 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 the Data Security Exhibit to this DPA. In addition, Stripe implements a data security incident management program that addresses how Stripe manages data security incidents, including any loss, theft, misuse, or unauthorized access, disclosure, or acquisition, or destruction, or other compromise of Personal Data ("**Incident**"). If Stripe is required by DP Law to notify User of an Incident, then Stripe will notify User without unreasonable delay, but in no event later than any time period required by the applicable DP Law. In addition, for Incidents affecting Personal Data subject to GDPR or UK GDPR, Stripe will notify User no later than 48 hours after Stripe becomes aware of the Incident. Stripe will partner with User to respond to the Incident. The response may include identifying key partners, investigation of the Incident, providing regular updates, and liaising with regards to notice obligations. Except as required by DP Law, Stripe will not notify User's affected Data Subjects about an Incident without first consulting User;

g. engage Sub-processors as necessary to perform the Stripe Services on the basis of the general written authorization User gives Stripe under Section 4.2 below;

h. to the extent required by DP Law and upon User's written request, contribute to audits or inspections by making audit reports available to User, which reports are Stripe's confidential information. Upon User's written request, and no more frequently than once annually, Stripe will promptly provide documentation evidencing its compliance with PCI-DSS and regarding Stripe's business practices and data technology environment in relation to its and its Affiliates' Processing of Personal Data. Stripe's responses to the security questionnaire are Stripe confidential information;

i. at User's choice, and subject to Stripe exercising its rights and performing its obligations under the Stripe Agreement, delete or return all Personal Data to User after the end of the provision of the Stripe Services, and delete existing copies, unless Stripe is required or authorized by DP Law to store Personal Data for a longer period; and

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

4.2 Sub-processors.

a. User specifically authorises the engagement of the Sub-processors from the agreed list of Sub-processors at stripe.com/service-providers/legal, which URL may be updated or replaced ("**Stripe Service Providers List**"). If User subscribes to email notifications at the Stripe Service Providers List, then Stripe will notify User via email of any changes Stripe intends to make to the Stripe Sub-processors List at least 30 days before the changes take effect. User may reasonably object to a change on legitimate grounds within 30 days after it receives notice of the change. User acknowledges that Stripe's Sub-processors are essential to provide the Stripe Services and that if it objects to Stripe's use of a Sub-processor, then notwithstanding anything to the contrary in the Stripe Agreement, Stripe will not be obligated to provide User the Stripe Services for which Stripe uses that Sub-processor.

b. Stripe will enter into a written agreement with each Sub-processor that imposes on the 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 User for the acts and omissions of its Sub-processor to the same extent Stripe would be liable if performing the relevant Stripe Services directly under this DPA.

4.3. Disclaimer of Liability. Stripe will not be liable for any claim brought by a Data Subject arising from or related to Stripe's or its Affiliate's action or omission to the extent that Stripe was acting in accordance with User's Instructions.

5. **User Obligations when acting as a Data Controller.** User will:

   a. only provide Instructions to Stripe that are lawful;

   b. comply with and perform all of its obligations under DP Law, including with regard to Data Subject rights, data security and confidentiality, and ensure it has an appropriate legal basis for the Processing of Personal Data as described in the Stripe Agreement and this DPA; and

   c. 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 User's Processing of Personal Data for the purposes described in the Stripe Agreement and this DPA.

6. **Data transfers.** To the extent necessary to provide the Stripe Services, Stripe or its Affiliate may transfer Personal Data Processed under this DPA outside the territory in which the Stripe Services are provided, subject to Stripe's compliance with DP Law. In respect of any transfers of Personal Data from the EEA, Switzerland or the UK to any third country that is not subject to an adequacy decision under DP Law, Stripe will implement appropriate safeguards, specified or permitted under DP Law, to ensure Stripe and its Affiliates comply with DP Law. User (as data exporter) may elect to enter into the Standard Contractual Clauses with Stripe, Inc. (as data importer).

7. **Term.** The term of this DPA begins on the Effective Date and terminates on the date on which the Stripe Agreement expires or terminates. Section 4.3 will survive termination of this DPA.

8. **Entire Agreement.** This DPA supersedes and replaces any data processing agreement in effect as of the Effective Date that governs the Processing of Personal Data by Stripe or its Affiliates in performing the Stripe Services for User or its Affiliates.

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

   a. the provisions of this DPA and the provisions of the Stripe Agreement, with respect to Personal Data Processing, the provisions of this DPA will prevail; and

   b. the provisions of the DPA and any provision contained in Standard Contractual Clauses executed by User and Stripe, Inc., the provisions of the Standard Contractual Clauses will prevail.

EXHIBIT: DATA SECURITY

Stripe	
Security Programs and Policies	Stripe maintains and enforces a security program that addresses the management of security and the security controls Stripe employs. The security program includes: ● documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually; ● documented, clear assignment of responsibility and authority for security program activities; ● policies covering, as applicable, acceptable computer use, data classification, cryptographic controls, access control, removable media, and remote access; and ● regular testing of the key controls, systems and procedures. **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. Stripe maintains and enforces an asset management program that appropriately classifies and controls hardware and software assets throughout their life cycle.
Worker Education and Worker Controls	All Stripe employees, agents, and contractors (collectively "**Workers**") acknowledge their data security and privacy responsibilities under Stripe's policies. For Workers who Process Personal Data, Stripe: ● implements pre-employment background checks and screening; ● conducts security and privacy training; ● implements disciplinary processes for violations of data security or privacy requirements; and ● upon termination or applicable role change, promptly removes or updates Worker access rights and requires the return or destruction of Personal Data. **Authentication**. Stripe authenticates each Worker'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 systems and applications that Process Personal Data.
Technical Access Controls	**Access control.** Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including:

	• user identification and authentication procedures; • ID/password security procedures (special characters, minimum length, change of password), including stronger digital authentication measures based on NIST 800-63b; • automatic blocking (e.g. password or timeout); and • monitoring of break-in-attempts. **Data access control.** Stripe implements measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including: • internal policies and procedures; • control authorization schemes; • differentiated access rights (profiles, roles, actions and objects); • monitoring and logging of accesses; • reports of access; • access procedure; • change procedure; and • 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 are processed, include: • physical access control system and program in place at Stripe premises; • 24x7 Global Security Operation Center monitoring physical security systems; • security video and alarm systems; • access control roles and area zones; • access control audit measures; • electronic tracking and management program for keys; • access authorizations process for employees and third parties; • door locking (electrified locks etc.); and • trained uniformed security staff. 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: • database replication; • backup procedures; • hardware redundancy; and • disaster recovery plan.
Disclosure Controls	Stripe implements measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it 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: ● "least privilege" limitation of access to data by internal service; ● segregation of functions (production/testing); ● procedures for storage, amendment, deletion, transmission of data for different purposes; and ● logical segmentation processes to manage the separation of Personal Data.
Certifications and Reports	**PCI Compliance**. Stripe will provide the Stripe 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). **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. 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 are restricted to a limited number of authorized Stripe personnel. **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 leverages encryption on all server infrastructure and production data stores using industry standard encryption (AES 256). **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 data security incidents, including any loss, theft, misuse, or unauthorized access, disclosure, or acquisition, or destruction, or other compromise of Personal Data. In accordance with its legal obligations, Stripe will notify impacted Stripe users and regulatory organizations (where applicable) of validated security incidents in a timely manner.
Reviews, Audit Reports, and	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

Security Questionnaires	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. 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. 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 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 such these policies and procedures as appropriate.