Data Processing Agreement

Last updated: September 28, 2026

1. Scope.

This Data Processing Agreement ("**DPA**") is between the Stripe entity specified in the Agreement (and its Affiliate(s), collectively "**Stripe**") and the User specified in the Agreement, and is subject to and incorporated by reference into the Agreement. This DPA governs Stripe's and its Affiliates' Processing of Personal Data.

2. Stripe as Data Processor and Data Controller.

Data Processing Roles	
Stripe as a Data Processor	When Stripe Processes Personal Data as a Data Processor, it is acting as a Data Processor on behalf of User, the Data Controller.
Stripe as a Data Controller	When Stripe Processes Personal Data as a Data Controller it: • has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through User; and • may engage a Stripe Affiliate to act as (a) a Joint Controller to provide products and services, including Authorized Services; (b) an independent Data Controller to provide Authorized Services; and (c) a Data Processor to provide services other than Authorized Services.
Data Processing Purposes	
Stripe as a Data Processor	The purposes of Stripe's Processing of Personal Data in its capacity as a Data Processor are to: • service the Stripe platform; and • provide, and provide access to, Stripe's products and services.
Stripe as a Data Controller	The purposes of Stripe's Processing of Personal Data in its capacity as a Data Controller when providing Stripe's products and services are to: • determine and utilize third parties (banks and payment method providers); • monitor, prevent and detect fraudulent transactions and other fraudulent activity on the Stripe platform; • monitor, prevent and mitigate financial loss, security risks, and other harm; • implement, maintain and perform internal processes that enable Stripe to provide its products and services, including relationship management, billing and invoicing; • comply with Law, including applicable anti-money laundering screening and know-your-customer obligations, and Financial Provider and Governmental Authority requirements and requests; and • analyze, improve and develop Stripe's products and services.
Categories of Data Subjects and Personal Data: Stripe as a Data Processor and a Data Controller	
Data Subjects	Stripe may Process the Personal Data of Customers, representatives and any natural person who accesses or uses the Stripe Account.

Personal Data	If applicable, Stripe may Process Payment Method Account Details, bank account details, billing/shipping address, name, order description (including date, time, amount, product or service description), 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), cryptocurrency wallet address.
Sensitive Data	If applicable, Stripe may Process Sensitive Data (e.g., facial recognition data).
Duration of Processing	
Stripe as a Data Processor	For the Term and any period required to perform a party's post-termination obligations.
Data Security	
Stripe as a Data Processor and Data Controller	Stripe will implement and maintain a written information security program with the Data Security Measures stated in the Exhibit of this DPA.

3. Stripe Obligations when Acting as a Data Processor.

3.1 Obligations.

When Stripe is acting as a Data Processor for User, Stripe will, to the extent required by DP Law:

(a) Process Personal Data on User's behalf and according to User's Instructions. Stripe will inform User if, in its opinion, Instructions violate or infringe DP Law;

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

(c) inform User of each request Stripe receives from Data Subjects (including "verifiable consumer requests" as defined under the CCPA) exercising their 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 (collectively "**Data Subject Request**"). Other than to request further information, identify the Data Subject, and, if applicable, direct the Data Subject to User as Data Controller, Stripe will not respond to these requests unless User instructs Stripe in writing to do so. Taking into account the nature of the Processing, Stripe will assist User by appropriate technical and organizational measures, insofar as this is possible, to enable User to meet its obligation to respond to a Data Subject Request;

(d) inform User of each law enforcement request Stripe receives from a Governmental Authority requiring Stripe to disclose Personal Data or participate in an investigation requiring Stripe to disclose Personal Data, unless prohibited by Law;

(e) provide User with reasonable assistance, following User's written request, to help User comply with its obligations under DP Law and, taking into account the nature of the Processing and the information available to Stripe, Stripe will provide reasonable information to help User conduct a data protection impact assessment or consult with a Supervisory Authority. If User requests assistance from Stripe that goes beyond Stripe's obligations under DP Law or this Agreement, Stripe may charge User a reasonable fee;

(f) if Stripe experiences a Data Incident, notify User without undue delay, which for Data Incidents affecting Personal Data subject to the GDPR or UK GDPR will be no later than 48 hours, in each case after becoming aware of the Data Incident. To the extent known to Stripe, Stripe's notification to User will describe in reasonable detail (i) the type of Personal Data that was the subject of the Data

Incident, (ii) the categories and potential number of individuals or records affected (including their countries), and (iii) the status of Stripe's investigation and current or planned remediation. Following the notification, Stripe will provide relevant updates to assist User in complying with its obligations under DP Law;

(g) following User's written request, contribute to audits or inspections by making audit reports available to User. Following this 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 reports and documentation provided, including any response to a security questionnaire, are Stripe's confidential information; and

(h) at User's choice, delete or return to User all Personal Data Processed in connection with the Services, and delete existing copies, following termination of the Agreement, except that Stripe will not be required to delete or return that Personal Data, or delete existing copies, to the extent that Stripe's storage of that Personal Data or those copies is (i) required by Stripe to exercise its rights and perform its obligations under this Agreement; or (ii) required or authorized by DP Law for a longer period.

3.2 Sub-processors.

(a) Stripe engages Sub-processors, which may include its Affiliates, as necessary to perform the Services. User consents to Stripe's use of its existing Sub-processors, as set out on the Stripe Sub-processors List, and grants Stripe a general written authorization to engage Sub-processors as necessary to perform the Services. If User subscribes to email notifications at the Stripe Sub-processors List, then Stripe will notify User via email if Stripe intends to add one or more Sub-processors to that list at least 30 days before the changes take effect. User may reasonably object to a change on legitimate grounds within 30 days after User receives notice of the change. User acknowledges that Stripe's Sub-processors are essential to provide the Services and that if User objects to Stripe's use of a Sub-processor, then notwithstanding anything to the contrary in the Agreement (including this DPA), Stripe will not be obligated to provide User 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 the obligation to implement 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 Services directly under this DPA.

3.3 United States Specific Data Protection Obligations.

To the extent that US State DP Law applies and Stripe is acting as a Data Processor, Stripe certifies that it understands and will comply with its obligations under US State Privacy Law to:

(a) not sell or share (as defined under the CCPA) Personal Data;

(b) only Process Personal Data for the purposes set out in this DPA, the Agreement or otherwise permitted by Law;

(c) not retain, use or disclose Personal Data outside of its direct business relationship with User other than to provide Stripe's products and services and as required to comply with Law; and

(d) not combine Personal Data received from or through User with Personal Data received from or on behalf of an individual or collected from Stripe's own interactions with the individual, unless permitted by US State DP Law or at the individual's direction.

(e) provide no less than the level of protection to Personal Data as required by US State DP Law; and

(f) inform User if it determines that it can no longer meet its obligations under the US State DP Law and will grant User the right to take reasonable and appropriate steps to remediate any unauthorized Processing of Personal Data.

3.4 Disclaimer of Liability.

Notwithstanding anything to the contrary in the Agreement, including 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 User's Instructions.

4. User's obligations when acting as a Data Controller.

4.1 Instructions.

User must only provide Instructions to Stripe that are lawful;

4.2 Compliance with DP Law.

User must comply with and perform User's obligations under DP Law, including with regard to Data Subject rights, data security and confidentiality, and ensure User has an appropriate legal basis for the Processing of Personal Data as described in the Agreement, including this DPA; and

4.3 Disclosures.

User must provide all necessary notices (including by making available a Privacy Policy) to, and obtain all necessary rights, permissions and consents from, Data Subjects (including Customers), to enable Stripe to lawfully Process any Personal Data provided by User as described in the Agreement, including this DPA. User is solely responsible for the content of notices it provides to its Customers.

5. Stripe's obligations when acting as a Data Controller.

Stripe must comply with and perform its obligations under DP Law when Processing Personal Data, including making available a Privacy Policy that explains how and for what purposes Stripe collects, uses, retains, discloses and safeguards Personal Data.

6. Data transfers.

6.1 Cross-border Data Transfers by User.

User acknowledges that in order for Stripe to provide the Services, User transfers Personal Data to Stripe, LLC in the United States. If the transfer comprises Personal Data that requires a Data Transfer Mechanism, the Data Transfers Addendum, which is incorporated into this DPA, will apply.

6.2 Cross-border Data Transfers by Stripe.

Stripe and its Affiliates may transfer Personal Data on a global basis as necessary to provide the Services. In particular, Personal Data may be transferred to Stripe, LLC in the United States and to Stripe's Affiliates and Sub-processors in other jurisdictions.

7. Conflict.

To the extent of any conflict between the provisions of this DPA and any provision of the:

(a) Agreement regarding Personal Data Processing, the provisions of this DPA will prevail; and

(b) Data Transfers Addendum, the provisions of the Data Transfers Addendum will prevail.

8. Definitions.

Capitalized terms not defined in this DPA have the meanings given to them in the Agreement.

"**Agreement**" has the meaning given in the Stripe services agreement between User and Stripe located at www.stripe.com/legal/ssa, or as otherwise agreed by the parties.

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

"**CCPA**" means California Consumer Privacy Act of 2018, Cal. Civ. Code Sections 1798.100-1798.199, and its implementing regulations.

"**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 Incident**" means an unauthorized or unlawful Processing, use, access, loss, disclosure, destruction or alteration of Personal Data in a party's or its Affiliate's, or a party's or its Affiliate's subcontractor's, agent's or representative's, possession or control.

"**Data Privacy Framework**" means, as applicable, the EU-US, Swiss-US or UK-US Data Privacy Framework self-certification program operated by the US Department of Commerce.

"**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.

"**Data Transfer Mechanism**" means a transfer mechanism that enables the lawful cross-border transfer of Personal Data under DP Law, which includes transfer mechanisms that are required under DP Law in the EEA, Switzerland and the UK, such as the Data Privacy Framework, the EEA SCCs, the UK International Data Transfer Addendum and any data transfer mechanism available under DP Law that is incorporated into this DPA.

"**Data Transfers Addendum**" means the data transfers addendum located at www.stripe.com/legal/dta, as updated from time to time.

"**DP Law**" means Law that applies to Personal Data Processing under the Agreement and this DPA, including international, federal, state, provincial and local Law relating in any way to privacy, data protection or data security.

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

"**EEA SCCs**" means Module 1 (Transfer: Controller to Controller), Module 2 (Transfer: Controller to Processor) and, as applicable, Module 3 (Transfer: Processor 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 General Data Protection Regulation (EU) 2016/679.

"**Instructions**" means any communication or documentation, including that which may be provided through a Stripe API, or Stripe Dashboard, or written agreements between User and Stripe through 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 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.

"**Privacy Policy**" means any or all of a publicly posted privacy policy, privacy notice, data policy, cookies policy, cookies notice or other similar public policy or public notice that addresses a party's Personal Data practices and commitments.

"**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. "**Processed**" and "**Processing**" have corresponding meanings.

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

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

"**Stripe Sub-processors List**" means the list of Stripe's Sub-processors and Affiliates located at www.stripe.com/legal/service-providers, as updated from time to time.

"**Supervisory Authority**" means an independent public authority which is (i) established by a European Union member state pursuant to Article 51 of the GDPR; or (ii) the public authority governing data protection that has supervisory authority and jurisdiction over User.

"**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.

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

"**US State DP Law**" means DP Law applicable in the United States, which may include, among others, the CCPA, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

EXHIBIT: STRIPE DATA SECURITY

Security Programs and Policies	Stripe maintains and enforces a security program that addresses how Stripe manages security, including its security controls. 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.

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. For Personnel, Stripe, either itself or through a third party: • 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 Personnel access rights and requires Personnel to return or destroy Personal Data. **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. Vulnerabilities are managed and remediated in accordance with Stripe's Vulnerability Management Standard.
Technical Access Controls	**Access control.** Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including the following measures: • user identification and authentication procedures; • ID/password security procedures, including stronger digital authentication measures based on NIST 800-63B including MFA; • automatic blocking (e.g., password or timeout); and • break-in-attempt monitoring. **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: • internal policies and procedures; • control authorization schemes; • differentiated access rights (profiles, roles, actions and objects); • access monitoring and logging; • access reports; • 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 is Processed, include: • physical access control system and program in place at Stripe premises; • 24x7 Global Security Operation Center that monitors 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 • 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: • "least privilege" limitation of access to data by internal services; • 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**. To the extent applicable to the Services, Stripe is responsible for providing 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). **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 is restricted to a limited number of authorized Personnel. **Encryption in transit.** To protect data in transit, Stripe requires all inbound and outbound data connections to be encrypted using cryptographic protocols, cipher suites, and key exchange mechanisms approved under current NIST guidelines. For data traversing Stripe's internal production networks, Stripe uses mutual authentication and encryption (mTLS) to secure connections between production systems. **Encryption at rest.** To protect data at rest, Stripe encrypts all production data stored in server infrastructure using encryption algorithms and key lengths that meet or exceed NIST recommendations for symmetric encryption.

	Payment Card and Banking Account Data Tokenization. Payment card and bank numbers are stored in a separate, highly restricted data vault and are separately encrypted at the data level using NIST-approved symmetric encryption algorithms and key lengths. Decryption keys are stored on separate machines. Tokens are generated to support Stripe data processing.
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. 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 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.