Agreement entered into between Stripe Payments Europe, Ltd., and Mathias Lorenzen, on 2020-08-29

Data Processing Addendum between Stripe and Stripe User

This Data Processing Addendum ("DPA") supplements your Stripe Agreement. Your Stripe Agreement is the Stripe Services Agreement, unless you have entered into another agreement with a Stripe entity with respect to your use of the Services (as that term is defined in your Stripe Agreement). This DPA applies to the extent you are using the Services in the context of your data processing activities that are subject to the EU General Data Protection Regulation ("GDPR").

This DPA is entered into by Stripe Payments Europe, Ltd. (referred to as "Stripe" in this DPA). Stripe Payments Europe, Ltd. is a subsidiary of Stripe, Inc., and is a private company incorporated in Ireland and registered with the Irish Data Protection Commissioner's Office. You must have an existing Stripe Account or be a party to a Stripe Agreement to accept this DPA on behalf of the legal entity that corresponds to your Stripe Account or Stripe Agreement. By clicking **"I accept"**, you agree to enter into this DPA with Stripe. Collectively, you and Stripe are referred to in this DPA as the "parties".

How to accept these terms:

To complete this DPA, you must click the "I accept" button below. Upon Stripe's receipt of a time-stamped acceptance via the Stripe website, this DPA will become legally binding between you and Stripe. If you do not have an existing Stripe Account, or are not a party to a Stripe Agreement, then you may not accept this DPA, and any attempt to do so will be void and of no effect.

1. General.

This DPA sets out data protection, security and confidentiality requirements with regard to the Processing of Personal Data (as each of these phrases is defined below) that is collected, disclosed, stored, accessed or otherwise processed by Stripe for the purpose of providing the Services.

2. Definitions.

When used in this DPA, these terms have the following meanings. Any capitalized terms not defined in this DPA have the meaning given in the Stripe Agreement.

"Applicable Law" means all applicable European Union ("EU") or national laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the European Union Data Protection Directive 95/46/EC, as amended or replaced, from time to time, such as by the General Data Protection Regulation 2016/679 ("GDPR"), with effect from 25 May 2018, and EU Member State laws supplementing the GDPR; the EU Directive 2002/58/EC ("e-Privacy Directive"), as amended or replaced from time to time, and EU Member State laws implementing the e-Privacy Directive, including laws regulating the use of cookies and other tracking means as well as unsolicited e-mail communications; EU Member State laws regulating security breach notification and imposing data security requirements; 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 of the Processing of Personal Data;

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller;

“Data Subject” means an identified or identifiable natural person to which the Personal Data pertain;

“Instructions” means this DPA and any further written agreement or documentation by way of which the Data Controller or its affiliates instruct the Data Processor to perform specific Processing of Personal Data;

“Personal Data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an 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 by Stripe for the purpose of providing the Services to you;

“Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“Pseudonymization” means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information;

“Sensitive Data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation; and

“Sub-processor” means the entity engaged by the Data Processor or any further Sub-processor to Process Personal Data on behalf and under the authority of the Data Controller.

3. Processing of Personal Data.

3.1 Stripe as a Data Processor. The parties acknowledge and agree that to the extent Stripe operates and manages an electronic commerce platform and facilitates payment transactions on your websites or applications, Stripe is acting as a Data Processor on your behalf, and you act as a Data Controller. Stripe will engage Sub-processors pursuant to the requirements set forth in Section 5 (“Sub-processors”) below.

3.2 Your Processing of Personal Data. You shall, in your use of the Services and provision of Instructions, Process Personal Data in accordance with the requirements of Applicable Law and provide Instructions to Stripe that are lawful. You shall ensure that Data Subjects are provided with appropriate information regarding the Processing of their Personal Data and, where required by Applicable Law, you shall obtain their consent to such Processing.

3.3 Stripe’s Processing of Personal Data. To the extent that Stripe is acting as a Data Processor, Stripe will: (a) Process Personal Data in accordance with the Instructions of the Data Controller and this DPA; (b) ensure that any person authorized by Stripe to Process Personal Data is committed to respecting the confidentiality of the Personal Data; (c) provide reasonable assistance to the Data Controller, at the expense of the Data Controller, in ensuring compliance with the obligations of the Data Controller under Applicable Laws, taking into account the nature of the Processing and the information available to the Data Processor; (d) contribute to audits or inspections conducted by Stripe’s authorized auditors by making available to the Data Controller upon reasonable request the respective audit reports (no more frequently than once per year) provided that the Data Controller enters into a non-disclosure agreement with Stripe regarding such audit reports; and (e) provide reasonable assistance to the Data Controller, upon request, and, at the expense of the Data Controller, facilitate the Data Controller’s compliance with its obligations in respect of conducting data protection impact assessments and consulting with a supervisory authority, as required by Applicable Law.

3.4 Details of the Processing. The subject-matter of Processing of Personal Data by Stripe is the performance of the Services pursuant to the Stripe Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in **Schedule A** to this DPA.

4. Rights of Data Subjects.

4.1 Data Subject Requests. Stripe will, to the extent permitted by Applicable Law or other applicable legal or regulatory requirements, inform you of any formal requests from Data Subjects exercising their rights of access, correction or erasure of their Personal Data, their right to restrict or to object to the Processing as well as their right to data portability, and will not to respond to such requests, unless instructed by you in writing to do so.

4.2 Assistance by Stripe. Stripe shall, upon your request, provide reasonable efforts to assist you in responding to such Data Subject requests, and to the extent legally permitted, you shall be responsible for any costs arising from Stripe's provision of such assistance.

5. Sub-Processors.

5.1 Appointment of Sub-Processors. You acknowledge and agree that: (a) Stripe affiliates may be retained as Sub-Processors; and (b) Stripe and Stripe affiliates may engage third-party Sub-Processors in connection with the provision of the Services. Stripe or a Stripe affiliate will enter into a written agreement with the Sub-Processor imposing on the Sub-Processor data protection obligations comparable to those imposed on Stripe under this Agreement with respect to the protection of Personal Data. In case the Sub-Processor fails to fulfill its data protection obligations under such written agreement with Stripe, Stripe will remain liable to you for the performance of the Sub-Processor's obligations under such agreement, except as otherwise set forth in the Stripe Agreement. By way of this DPA, the Data Controller provides general written authorization to Stripe as Data Processor to engage Sub-Processors as necessary to perform the Services.

5.2 List of Current Sub-Processors. Stripe shall make available a list of Sub-Processors for the Services. A current list of the Stripe Sub-Processors can be found here. Stripe will update the list to reflect any addition, replacement or other changes to Stripe's Sub-Processors.

5.3. Objection Right for New Sub-Processors. You may reasonably object to Stripe's use of a new Sub-Processor on legitimate grounds, subject to the termination and liability clauses of the Stripe Agreement. The Data Controller acknowledges that these Sub-Processors are essential to providing the Services and that objecting to the use of a Sub-Processor may prevent Stripe from offering the Services to the Data Controller.

6. Security.

6.1 Controls for the Protection of Personal Data. Each party shall implement and maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data, including, where appropriate: (a) Pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services involved in the processing of Personal Data; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data.

6.2 Personal Data Incident Management and Notification. Stripe will implement and maintain a data security incident management program, compliant with Applicable Law, that addresses management of

data security incidents including a loss, theft, misuse, unauthorized access, disclosure, or acquisition, destruction or other compromise of Personal Data ("Incident"). Except to the extent necessary to comply with applicable legal, regulatory or law enforcement requirements, Stripe will inform you without unreasonable delay in accordance with Applicable Law after it becomes aware of any Incident that has occurred in its systems which affects Personal Data Stripe processes on your behalf.

7. Return and Deletion of Customer Data.

Stripe will delete or return all Personal Data to the Data Controller at the end of the provision of the Services, and delete existing copies, unless further storage of the Personal Data is required or authorized by Applicable Law.

8. Data Transfers

8.1 Data Transfer Mechanism. The parties agree that Stripe may transfer Personal Data processed under this DPA outside the European Economic Area ("EEA"), the UK or Switzerland as necessary to provide the Services. If Stripe transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission or the UK (as applicable) has not issued an adequacy decision, Stripe will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Applicable Law.

8.2 Stripe's Privacy Shield Certification. Stripe transfers Personal Data processed under this DPA to Stripe Inc. under the Privacy Shield certification of Stripe Inc., available at www.privacyshield.gov/list. For Stripe's Privacy Shield policy, please visit stripe.com/privacy-shield-policy.

9. Stripe's Role as Data Controller.

The Parties acknowledge and agree that to the extent Stripe processes Personal Data involved in payment transactions to: (1) monitor, prevent and detect fraudulent payment transactions, and to prevent harm to you, Stripe and the Stripe affiliates, and to third parties; (2) comply with legal or regulatory obligations applicable to the processing and retention of payment data to which Stripe is subject, including applicable to the processing and retention of payment data to which Stripe is subject, including applicable anti-money laundering screening and compliance with know-your-customer obligations ("AML & KYC Obligations"); (3) analyze, develop and improve Stripe's products and services; and (4) provide the Stripe products and services to Stripe users, Stripe is acting as a Data Controller with respect to the Processing of Personal Data it receives from or through you.

10. Termination.

This DPA will have the same duration as and will be subject to the termination terms of the Stripe Agreement. The obligations of Stripe to implement appropriate security measures with respect to Personal Data will survive the termination of this DPA and will apply for so long as Stripe retains Personal Data. In the event of a conflict between this DPA and the Stripe Agreement, this DPA will apply to the extent of the inconsistency.

11. Limitation of Liability.

Each party's (including their respective affiliates') liability, in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Stripe Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Stripe Agreement and all DPAs together.

DPAs together.

12. Governing Law.

This DPA and any dispute or claim arising out of or in connection with this DPA or its subject matter shall be governed by, and construed in accordance with, the laws of Ireland.

Schedule A: Description of Processing where Stripe acts as a Data Processor

Subject Matter: Stripe's provision of the Services to you.

Duration of Processing: For the duration of the term of the Stripe Agreement, plus the period from the expiration of the Stripe Agreement while Personal Data is retained.

Data Subjects: Consumers and cardholders.

Data Processing Activities: Managing an e-Commerce platform and facilitating payment transactions on behalf of Stripe users.

Categories of Personal Data: Personal data necessary to manage the electronic commerce platform and to process payment transactions such as:

- cardholder name
- email address
- unique customer identifier
- order ID
- bank account details
- payment card details
- card expiration date
- CVC code
- date/time/amount of transaction
- merchant name/ID
- location

Stripe does not knowingly process Sensitive Data in the context of the processing activities described in this Schedule.

Agreement entered into between Stripe Payments Europe, Ltd., and Mathias Lorenzen, on 2020-08-29