# DATA PROCESSING AGREEMENT (DPA)

| | |
|---|---|
| **Stripe** | Stripe Payments Europe, Ltd., a private limited company organized under the laws of Ireland with company number 513174 and offices at The One Building, 1 Grand Canal Street Lower, Dublin 2, Ireland |
| **User** | Leocare , a SASU,6 R DU GENERAL BERTRAND PARIS |
| **Effective Date** | 6/4/2021 |
| **Stripe Agreement** | Stripe Services Agreement located at https://stripe.com/[countrycode]/legal, where "country code" means the two-letter abbreviation for the country where User is located |

**SIGNATURES**

| **Stripe** | **User** |
|---|---|
| Emma Redmond<br>By: Emma Redmond | DocuSigned by:<br>51B262372C164E7...<br>By: Noureddine Bekrar |

## SCOPE

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

Stripe and User agree as follows:

1. **Structure.** This DPA states the privacy, data protection and security requirements that apply to Stripe's Processing of Personal Data for the purpose of providing the Stripe Services to User under the Stripe Agreement. In addition, Stripe and User intend that, 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, that this DPA states the terms that will apply to those parties in those regions, 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 them in the Stripe Agreement.

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

   "**DP Law**" means all laws and regulations that apply to Personal Data Processing under the 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 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 of the Processing of 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 pertain.

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

"**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 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.

"**Sub-processor**" means an entity engaged by the Data Processor (or any Sub-processor of the Data Processor) to Process Personal Data on behalf and under the authority of the Data Controller.

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

To the extent Stripe Processes Personal Data as:

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

b. a Data Controller (as specified in the table below), Stripe 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. |
| **Sensitive Data** |
| Where applicable, facial recognition data. |
| **Data Processing Purposes:** |

| Stripe as Data Processor | Stripe as Data Controller |
|---|---|
| • Servicing the Stripe platform;<br>• 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);<br>• Monitoring, preventing and detecting fraudulent payment transactions and other fraudulent activity on the Stripe platform;<br>• Determining the means and purposes of processing to comply with legal obligations that apply to the financial sector to which Stripe is subject, including applicable anti-money laundering screening and know-your-customer obligations;<br>• Analyzing and developing Stripe's products and services. |

4. **Stripe Obligations when acting as a Data Processor.** To the extent that Stripe is acting as a Data Processor for User, the Data Controller, 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 Law, 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 of access to (right to know to under the CCPA), or correction or erasure of, their Personal Data, their right to restrict or object to Stripe's Processing, or their right to 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 to 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 set out 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, 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 nature of the collaboration means 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 given by User to Stripe under this DPA. Stripe will inform User if it adds, replaces, or changes its Sub-processors by updating the Services Providers List at stripe.com/service-providers/legal. User has the opportunity to reasonably object to the changes on legitimate grounds within 30 calendar days after the change. User acknowledges that these Sub-processors are essential to provide the Stripe Services and that if it objects to Stripe's use of a Sub-processor, then Stripe will not be obligated to provide User the Stripe Services for which Stripe uses that Sub-processor. 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. In case a Sub-processor fails to fulfill its data protection obligations under that agreement, Stripe will remain liable to User for the performance of the Sub-processor's obligations under that agreement;

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. subject to DP Law, 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. not be liable for any claim brought by a Data Subject arising from any action or omission by Stripe or its Affiliate, to the extent that the action or omission resulted from User's Instructions.

k. 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.

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. ensure that it provides Data Subjects with all necessary information (including by means of offering a transparent and easily accessible public privacy notice) regarding the Processing of Personal Data by User and Stripe, respectively, for the purposes described in the Stripe Agreement and this DPA.

6. **Data transfers.** To the extent necessary to provide the Stripe Services, Stripe may transfer Personal Data that Stripe Processes under this DPA outside the territory in which the Stripe Services are provided, subject to Stripe's compliance with DP Law. If Stripe transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission, Switzerland or the UK (as applicable) has not issued an adequacy decision, Stripe will implement appropriate safeguards as required, including Standard Contractual Clauses as applicable, to transfer Personal Data in accordance with DP Law.

7. **Term.** The term of this DPA begins on the Effective Date and terminates on the date on which the Stripe Agreement has expired or terminated.

8. **Entire Agreement.** This DPA supersedes and replaces any data processing agreements between the parties that are in place as of the Effective Date and govern Personal Data Stripe processes in performing the Stripe Services.

# Exhibit: Data Security

**1. Programs and Policies.**

a. **Security Program.** Stripe maintains and enforces a security program that addresses how Stripe manages its security and employs security controls. Stripe's security program includes: (i) documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually; (ii) documented, clear assignment of responsibility and authority for security program activities; (iii) policies covering, as applicable, acceptable computer use, access control, and remote access; and (iv) regular testing of Stripe's key controls, systems and procedures.

b. **Privacy Program.** Stripe maintains and enforces a privacy program and related policies that address how Stripe collects, uses and shares Personal Data.

**2. Risk and Asset Management.**

a. **Risk Management.** Stripe performs risk assessments and implements and maintains controls for risk identification, analysis, monitoring, reporting, and corrective action.

b. **Asset Management.** Stripe maintains and enforces an asset management program that appropriately classifies and controls hardware and software assets throughout their life cycle.

**3. Worker Education.**

a. **Workers**. All Stripe employees, contractors and agents (collectively "**Workers**") acknowledge their data security and privacy responsibilities under Stripe's policies.

b. **Worker Controls**. For Workers who Process Personal Data, Stripe: (i) performs pre-employment background checks and screening; (ii) conducts security and privacy training; (iii) implements disciplinary processes for violations of data security or privacy requirements; and (iv) upon termination or applicable role change, promptly removes or updates Worker access rights and requires the Worker to return or destroy Personal Data in the Worker's possession or under the Worker's control.

**4. Network and Operations Management.**

a. **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.

b. **Vulnerability Assessments.** Stripe performs periodic vulnerability assessments and penetration testing on systems and applications that Process Personal Data.

**5. Access Control.**

a. **Access Control**. Stripe implements access controls designed to maintain the confidentiality of Personal Data. These controls include: (i) authorization processes for physical, privileged, and logical access to facilities, systems, networks (including wireless networks), operating systems, Stripe managed endpoints , system utilities, and other locations containing Personal Data; and (ii) granting access only if it is logged, strictly controlled, and needed for a Worker to perform their job function.

b. **Authentication**. Stripe authenticates each Worker's identity through appropriate authentication credentials such as strong passwords, token devices, or biometrics.

**6. PCI Compliance**. Stripe will provide the Stripe Services in a manner that is at all times consistent with the highest certification level (PCI Level 1) provided by the Payment Card Industry Data Security Standard requirements ("**PCI-DSS**"). Stripe's certification will be confirmed annually by a qualified security assessor (QSA).