

## DATA PROTECTION ADDENDUM

This Data Protection Addendum ("DPA") forms part of the Agreement between Chargehound LLC ("Chargehound") and Merchant, to reflect the parties' agreement with regard to the Processing of Personal Data. All capitalized terms not defined shall have the meaning set forth in the Agreement. In the event of any inconsistency between this DPA and the Agreement (including any other exhibits or schedules thereto), this DPA will prevail to the extent of such inconsistency. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules.

### 1. DEFINITIONS

"**Merchant**" means the entity identified on the signature lines of the Agreement or its Affiliates.

"**CCPA**" means the California Consumer Privacy Act of 2018, Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, as amended by the California Privacy Rights Act of 2020 ("**CPRA**"), including any applicable regulations thereunder, as the same may be amended from time to time.

"**Customer**" means a customer of Merchant and for the purposes of this DPA is a data subject.

"**Customer Data**" means the Personal Data that the Customer provides to Merchant and Merchant passes on to Chargehound through the use by the Merchant of the Services.

"**Data controller**" (or simply "controller"), "**data processor**" (or simply "processor"), "**data subject**" or terms addressing similar data protection and privacy roles have the meanings given to those terms under the Data Protection Laws.

"**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement as amended from time to time.

"**Data Subject Right**" means any right afforded to a Data Subject under Data Protection Laws, including the rights to access, rectify, restrict the processing of personal data, erasure (including the right to be forgotten), data portability, objecting to the processing, or to not be subject to an automated individual decision making.

"**PayPal Group**" means PayPal and all companies in which PayPal or its successor directly or indirectly from time to time owns or controls.

"**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 a name, an identification number, location data, an online identifier, or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person, or is otherwise "personal data," "personal information," "personally identifiable information," or similar designation under and regulated by Data Protection Laws.

"**Processing**" (including "process", "processes" and "processed") means any operation or set of operations which is performed upon personal data, whether or not by automatic means, 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.

"**Security Incident**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data on systems managed by or otherwise controlled by Chargehound or its Sub-processors of which Chargehound becomes aware.

**"Standard Contractual Clauses" or "SCCs"** means the "Controller to Processor" module of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

**"Sub-processor"** means any processor engaged by Chargehound and/or its authorized affiliates in the processing of personal data.

## 2. PROCESSING OF PERSONAL DATA

**2.1 Data Controller.** With regard to any Customer Data to be processed by Chargehound in connection with the Agreement, Merchant will be the controller and Chargehound will be the processor in respect of such processing. Merchant will be solely responsible for determining the purposes for which and the manner in which Customer Data are, or are to be, processed by Chargehound. Merchant shall have sole responsibility for the accuracy, quality, and legality of personal data and the means by which Customer acquired the Personal Data.

**2.2 Merchant Written Instructions.** Chargehound shall only process Customer Data on behalf of and in accordance with Merchant's written instructions. The Parties agree that this DPA constitutes Merchant's complete and final written instruction to Chargehound in relation to Customer Data. Additional instructions outside the scope of this DPA (if any) require prior written agreement between Chargehound and Merchant, including agreement of any additional fees payable by Merchant to Chargehound for carrying out such additional instructions. Merchant shall ensure that its instructions comply with all applicable laws, including Data Protection Laws, and that the processing of Customer Data in accordance with Merchant's instructions will not cause Chargehound to be in breach of Data Protection Laws. The provisions of this Section are subject to the provisions of Section 6 on Security. Merchant hereby instructs Chargehound to process Customer Data for the following purposes:

- (a) as reasonably necessary to provide the Chargehound Services to Merchant;
- (b) to monitor, prevent and detect fraudulent transactions and to prevent harm to Merchant and Chargehound;
- (c) to comply with legal or regulatory obligations applicable to the Chargehound Services to which Chargehound is subject.
- (d) to analyze, debug, to identify and repair errors that impair intended functionality;
- (e) to develop, enhance, and improve Chargehound's Services on behalf of the Merchants; and
- (f) after anonymizing the Customer Data, to use the anonymized Customer Data in accordance with applicable laws.

**2.3 Chargehound Cooperation.** In relation to Customer Data processed by Chargehound under the Agreement, Chargehound shall cooperate with Merchant to the extent reasonably necessary to enable Merchant to adequately discharge its responsibility as a controller under Data Protection Laws, including as Merchant requires in relation to:

- (a) assisting Merchant in the preparation of data protection impact assessments related to Merchant's use of the Services to the extent (i) required of Merchant under Data Protection Laws and/or (ii) Merchant does not otherwise have access to the relevant information and to the extent such information is available to Chargehound; and
- (b) responding to binding requests from data protection authorities for the disclosure of Customer Data as required by applicable laws.

**2.4 Scope and Details of Customer Data processed by Chargehound.** The objective of processing Customer Data by Chargehound is the performance of the Services pursuant to the Agreement. Chargehound shall process the Customer

Data in accordance with the specified duration, purpose, type and categories of data subjects as set out in Annex 1 (Data Processing of Customer Data), as applicable, the Agreement and this DPA.

**2.5 Compliance with Laws.** The Parties will at all times comply with Data Protection Laws.

### **3. RIGHTS OF DATA SUBJECTS**

**3.1 Data Subject Requests.** Chargehound shall, to the extent legally permitted and to the extent Chargehound is able to identify that the request comes from a data subject whose Personal Data was submitted to the Services by Merchant, promptly notify Merchant if it receives a request from a Customer for exercising Data Subject Rights in relation to that Customer's Personal Data. Chargehound may confirm to the data subject that it has passed the request to Merchant, however, Merchant shall be responsible for responding to all such requests and Chargehound will not respond or take action in relation to such requests, unless instructed by Merchant in writing to do so. If legally permitted, Chargehound shall provide Merchant with commercially reasonable cooperation and assistance regarding such Customer's request and Merchant shall be responsible for any costs arising from Chargehound's assistance.

**3.2** To the extent Merchant, in its use of the Chargehound Services, does not have the ability to fulfill the Customer's request for exercising Data Subject Rights in relation to Customer Data, as required by Data Protection Laws, Chargehound shall comply with any commercially reasonable request by Merchant to facilitate the required actions to the extent Chargehound is legally permitted to do so.

### **4. CHARGEHOUND PERSONNEL**

**4.1 Training.** Chargehound undertakes to provide training as necessary from time to time to Chargehound's personnel with respect to Chargehound's obligations under this DPA to ensure that Chargehound's personnel are aware of and comply with such obligations.

**4.2 Confidentiality and Limitation of Access.** Chargehound shall ensure that its personnel and other persons engaged in the Processing of Personal Data have committed themselves to confidentiality. Chargehound shall ensure that access by Chargehound's personnel to Customer Data is limited to those personnel performing Services in accordance with the Agreement and Data Protection Laws.

### **5. SUB-PROCESSORS.**

**5.1 Appointment of sub-processors.** For the purposes of the Agreement, in addition to those sub-processors specified at the following link: [www.chargehound.com/security](http://www.chargehound.com/security), Merchant specifically authorizes the engagement of members of the PayPal Group as sub-processors in connection with providing and improving Chargehound's Services. Chargehound shall enter into written contracts with all sub-processors, which contain terms for the protection of Customer Data in accordance with Data Protection Laws and which are no less protective than the terms set out in this DPA. When engaging a sub-processor not previously specified, Chargehound will provide prior notice by email to Merchant before implementing such change.

**5.2 Right to object.** If Merchant has a reasonable basis to object to Chargehound's use of the new sub-processor, Merchant shall notify Chargehound promptly in writing within ten (10) days after receipt of Chargehound's notice. In the event Merchant objects to a new sub-processor(s) and that objection is not unreasonable, Chargehound will use reasonable efforts to make available to Merchant a change in the affected Services or recommend a commercially reasonable change to Merchant's configuration or use of the affected Services to avoid processing of Personal Data by the objected-to new sub-processor without unreasonably burdening Chargehound. If Chargehound is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Merchant may terminate the

Agreement in respect only of those Services which cannot be provided by Chargehound without the use of the objected-to new sub-processor, by providing no less than thirty (30) days' written notice to Chargehound.

## 6. SECURITY

**6.1 Control and Protection of Customer Data.** Chargehound shall, at a minimum, implement and maintain appropriate technical and organizational measures as described in Annex 2 to this DPA to keep Customer Data secure and protect it against unauthorized or unlawful processing and accidental loss, destruction or damage in relation to the provision of the Services. Merchant understands and agrees that the technical and organizational measures are subject to technical progress and development. In that regard, Chargehound is expressly permitted to implement adequate alternative measures as long as Chargehound does not materially decrease the overall security level of the measures maintained in relation to the provision of the Services.

**6.2 Security Incident Notification.** If Chargehound becomes aware of a Security Incident in connection with the processing of Customer Data, Chargehound will, in accordance with Data Protection Laws: (a) notify Merchant of the Security Incident promptly and without undue delay after becoming aware of such Security Incident; (b) promptly take reasonable steps to minimize harm and secure Customer Data; (c) describe, to the extent possible, reasonable details of the Security Incident, including steps taken to mitigate the potential risks; and (d) deliver its notification to Merchant's administrators by email and Merchant is solely responsible for maintaining accurate contact information and ensuring that any contact information is current and valid. Chargehound shall make commercially reasonable efforts to identify the cause of such Security Incident and take those steps as Chargehound deems necessary and reasonable in order to remediate the cause of such Security Incident to the extent the remediation is within Chargehound's reasonable control. Chargehound's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Chargehound of any fault or liability with respect to the Security Incident. The obligation to remediate the cause of a Security Incident shall not apply to Security Incidents that are caused by Merchant. Merchant must notify Chargehound promptly about any possible misuse of Merchant's accounts or authentication credentials or any Security Incident related to the Services.

### 6.3 Audits and Certifications.

Where requested by Merchant in writing and occurring no more than one (1) time per calendar year, with at least three (3) weeks' advance notice and subject to the confidentiality obligations set forth in the Agreement, Chargehound shall make available to Merchant (or Merchant's independent, third-party auditor that is not a competitor of Chargehound, PayPal or any members of the PayPal Group and that is subject to confidentiality obligations substantially similar to those set forth in the Agreement) information regarding Chargehound's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits which shall consist of Chargehound's provision of written information about its security policies, and interviews with Chargehound's IT personnel.

Chargehound shall:

- (a) provide reasonable access to data and information reasonably required for the conducting of such an audit or inspection;
- (b) take all reasonably necessary steps to comply with the terms of the Agreement and this DPA if the result of an audit demonstrates that Chargehound is failing to comply with any of its obligations under the Agreement or this DPA; and
- (c) provide status reports regarding Chargehound's resolution of any audit-related compliance activity for which it is responsible.

Merchant shall:

- (a) promptly notify Chargehound with information regarding any non-compliance discovered during the course of an audit. If the auditor's report reveals that: (a) a material breach of Chargehound's obligations under this DPA or the Agreement; or (b) that the technical and organizational safeguards adopted pursuant to Section 6.1 are materially inadequate, then Chargehound must take reasonable steps to ensure that any such breach does not reoccur or that the systems and procedures are rectified, as the case may be;
- (b) provide Chargehound a copy of any final audit report upon Chargehound's request, unless prohibited by applicable Data Protection Laws; and
- (c) treat the findings of any final audit report as Confidential Information in accordance with the terms of the Agreement, and use it solely for the purpose of assessing Chargehound's compliance with the terms of the Agreement, this DPA and Data Protection Laws.

**7. DELETION AND RETURN OF MERCHANT DATA.**

Upon termination or expiry of the Agreement, Chargehound will at the choice of the Merchant, delete or return to Merchant all Customer Data processed on behalf of the Merchant, and Chargehound shall delete existing copies of such Customer Data except where authorized by Data Protection Laws or necessary to retain such Customer Data strictly for the purposes of compliance with applicable law.

**8. TRANSFER MECHANISM FOR DATA TRANSFER.**

[Intentionally Omitted]

**9. CCPA SPECIFIC PROVISIONS**

**9.1 Application.** The Parties agree that the provisions of this Section apply to any Personal Information (as defined under the CCPA) Processed on behalf of Merchant:

**9.2. Definitions.**

**Data Protection Laws.** All references to Data Protection Laws in this DPA include a reference to the CCPA;

**Personal Information.** All references to Personal Data in this DPA include Personal Information, as defined in the CCPA;

**Businesses.** All references to "Controller" in this DPA include a reference to "Business," as defined in the CCPA;

**Service Providers.** All references to "Processor" in this DPA include a reference to "Service Provider," as defined in the CCPA;

**Capitalized Terms.** Capitalized terms used in this Section that are not defined in this Section have the meaning set forth in the CCPA.

**9.3 Specified Business Purpose.** The Parties acknowledge and agree that the applicable Business Purposes are the processing purposes described in Section 2.2 of this DPA and any business purposes permitted under the CCPA (collectively, the "Specified Business Purpose").

**9.4 Disclosure of Information.** Merchant discloses Personal Information to Chargehound only for the Specified Business Purpose.

- 9.5 Processing Limitation.** Chargehound shall Process Personal Information on behalf of Merchant to the extent required to perform the Specified Business Purpose, and shall not retain, use, or disclose Personal Information for any purpose (including a commercial purpose) other than the Specified Business Purpose or outside of the direct business relationship between it and Merchant.
- 9.6 No Selling or Sharing.** Chargehound shall not Sell or Share any Personal Information for any reason. Chargehound does not receive any Personal Information from Merchant as consideration for Chargehound's provision of the Services.
- 9.7 Combining Information.** Chargehound shall not combine Personal Information with any other information it (A) receives from or on behalf of another person or third party or (B) collects from its own interactions with the applicable data subject, except to perform a Business Purpose within the limits of the CCPA.
- 9.8 Use of Personal Information.** Merchant can take reasonable and appropriate steps: (i) to help to ensure that Chargehound uses Personal Information in compliance with Merchant's obligations under the CCPA; and (ii) upon notice, to stop and remediate any unauthorized use of Personal Information.
- 9.9 Notification.** Chargehound shall promptly, and without undue delay, notify Merchant if Chargehound determines it can no longer meet its obligations to Merchant under the CCPA.
- 9.10 Certification.** Chargehound certifies that it understands the restrictions set forth in this DPA, including specifically this Section.
- 10. MISCELLANEOUS.**
- 10.1** In the event of inconsistencies between the provisions of this DPA and other agreements between the parties except the SCCs, the provisions of this DPA shall prevail with regard to the parties' data protection obligations relating to Customer Data. In cases of doubt, this DPA shall prevail, in particular, where it cannot be clearly established whether a clause relates to a party's data protection obligations.
- 10.2** Should any provision or condition of this DPA be held or declared invalid, unlawful or unenforceable by a competent authority or court, then the remainder of this DPA shall remain valid. Such an invalidity, unlawfulness or unenforceability shall have no effect on the other provisions and conditions of this DPA to the maximum extent permitted by law. The provision or condition affected shall be construed either: (a) to be amended in such a way that ensures its validity, lawfulness and enforceability while preserving the parties' intentions, or if that is not possible, (b) as if the invalid, unlawful or unenforceable part had never been contained in this DPA.
- 10.3** Any amendments to this DPA shall be in writing duly signed by authorized representatives of the parties hereto.

List of Annexes:

Annex 1: Details of the Processing

Annex 2: Technical and Organizations Measures Including Technical and Organizational Measures to Ensure the Security of the Data

## ANNEX I

### A. List of Parties

#### Data Exporter

- Name and Address: The data exporter is the Merchant and the address is as provided in the Agreement
- Contact person's name, position and contact details: as provided in the Agreement
- Activities relevant to the data transferred under the Standard Contractual Clause: as provided in the Agreement
- Signature and date: please see the "Transfer Mechanism for Data Transfer" section of Schedule 1
- Role (controller/processor): controller

#### Data Importer

- Name and Address: The data importer is Chargehound and the address is as provided in the Agreement
- Contact person's name, position and contact details: as provided in the Agreement
- Activities relevant to the data transferred under the Standard Contractual Clause: as provided in the Agreement
- Signature and date: please see the "Transfer Mechanism for Data Transfer" section of Schedule 1
- Role (controller/processor): processor

### B. DESCRIPTION OF TRANSFER

#### Categories of data subjects Whose Personal Data is Transferred

Customer Data – The Personal Data that the Customer provides to Merchant and Merchant passes on to Chargehound through the use by the Merchant of the Services.

#### Categories of Personal Data Transferred

Customer Data – Merchant shall inform Chargehound of the type of Customer Data Chargehound is required to process under the Agreement. Should there be any changes to the type of Customer Data Chargehound is required to process then Merchant shall notify Chargehound immediately.

The relevant categories of Personal Data that are the subject of this DPA and these Standard Contractual Clauses is data relating to individuals using data exporter's services and provided by the data exporter, which may include, but is not limited to the following categories of Personal Data:

First name

Last name

Address

Phone number

Email address

IP address

Payment information

Any other Personal Data or information that Merchant decides to provide to Chargehound.

### **Sensitive Data Transferred (if appropriate) and Applied Restrictions or Safeguards**

The personal data transferred concern the following categories of sensitive data:

The transfer of sensitive data is not anticipated.

Applies restrictions and safeguards:

- Not applicable.

### **Nature of the Processing**

As set forth in the Agreement.

### **Purpose(s) of the Transfer(s)**

The transfer is made for the following purposes:

- Performance of the Services provided by data importer to data exporter in accordance with the Agreement.
- To comply with laws applicable to the data importer.
- As set forth in Schedule 1, the Data Protection Addendum

### **The frequency of the transfer:**

Data exporter will transfer the data for the term set forth in the Agreement.

### **The Period for which the Personal Data will be Retained, or, if that is not Possible, the Criteria Used to Determine that Period**

The data importer only retains the personal data for as long as is necessary with regards the relevant purpose(s) it was collected for (please see purposes above). To determine the appropriate retention period for personal data, the data importer considers the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of the personal data, the purposes for which the personal data is processed and whether such purposes can be achieved through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

### **For transfers to (Sub-) Processors, also Specify Subject Matter, Nature and Duration of the Processing**

The data importer may share personal data with third-party service providers that perform services and functions at the data importer's direction and on its behalf. These third-party service providers may, for example, provide an element of the services provided under the Agreement such as customer verification, transaction processing or customer support, or provide a service to the data importer that supports the Services provided under the Agreement such as storage. When determining the duration of the processing undertaken by the third-party service providers, the data importer applies the criteria provided above in this Annex 1.

### **C. Supervisory Authority**

In accordance with Clause 13(a) of the EU Transfer Clauses, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated shall act as competent supervisory authority.

## ANNEX II

### Technical and Organizations Measures Including Technical and Organizational Measures to Ensure the Security of the Data

**1. Pseudonymization, Encryption and the Protection of Data During Transmission.**

Chargehound encrypts data in transit and at rest.

**2. Regular Testing, Assessment and Evaluating Effectiveness of Technical and Organizational measures.**

Chargehound regularly plans and executes the Company's testing program to assess and evaluate the effectiveness of its technological and organizational measures.

**3. User Identification and Authorization.**

Chargehound restricts access to the Company network and any in-scope applications through use of unique corporate network account IDs and passwords for user identification and authentication.

**4. Physical Security of Locations Where Personal Data is Processed.**

Chargehound's safety and security policies and processes set forth the requirements necessary to facilitate safety and security processes, including physical security, in accordance with applicable laws, regulations and partner requirements.

**5. IT Governance and Management; Certification and Assurance of Processes and Products.**

Chargehound promotes a strong security philosophy across the Company. Chargehound's Information Security Program is designed to support the Company in managing technology and information security risks and identifying, protecting, detecting, responding to and recovering from information security threats. Chargehound certifies and assures its processes and products against industry standards through a variety of programs, including an annual SOC 2, type 2 assessment.

**6. Data Minimization.**

Our policies require, that data elements collected and generated are those which are adequate, relevant, and limited in relation to the purposes for which they are processed, and Chargehound implements technical controls to enforce these policies where applicable.

**7. Events Logging and Configuration.**

Chargehound collects and maintains event and system configuration logging to support security, privacy and data issue and incident detection, investigation, remediation and recovery efforts.

**8. Data Quality and Retention.**

Chargehound monitors data quality, issues and remediations, as necessary. Data is classified according to its business value and Chargehound has defined retention periods based upon Chargehound's legal, regulatory, and business recordkeeping requirements. Upon expiration of an applicable retention period, data and information is disposed, deleted, or destroyed.

**9. Accountability.**

Chargehound has developed a set of policies and principles that are aligned to industry standards and designed to engage stakeholder collaboration and partnership in awareness and compliance with such policies and controls across the organization to ensure participation and accountability from the top down across the organization. Chargehound complies with the relevant articles carrying an accountability obligation in the GDPR and other applicable data protection laws.

**10. Data Subject Rights.**

Chargehound supports merchants in fulfilling their data subject rights obligations, including access, correction and erasure, and provides a suite of tools to facilitate this process for merchants. Such support is provided except for circumstances in which Chargehound has an overriding legal or regulatory obligation or other legitimate business purpose that prohibits it from doing so.

**11. Processors.**

Chargehound contractually requires its service providers, processors, and their subprocessors to put in place comprehensive data security and privacy standards throughout the processing chain.