DATA PROTECTION ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the Hyperswitch Merchant Agreement ("**Agreement**") entered by and between the Merchant and Juspay (Processor).

This Addendum reflects the Parties' desire and intent to modify and amend the Agreement, in accordance with the terms and conditions hereinafter set forth, with regards to the processing of Personal Data (as defined below) by Processor on behalf of Merchant.

Processor and the Merchant are sometimes hereinafter collectively referred to as the "**Parties**" and individually as a "**Party**".

Section 1 Scope, Order of Precedence, and Term

(a) This Addendum modifies and supplements the terms and conditions in the Agreement as they relate to Juspay's Processing of Personal Data and compliance with Data Protection Law. Notwithstanding anything to the contrary in the Agreement, if there is a conflict between Agreement and the Addendum, this Addendum will control. This Addendum will be attached to and incorporated into the Agreement.

(b) This Addendum applies only to the extent that Juspay receives, stores, or Processes Personal Data in connection with the Services described in this Addendum.

Section 2 Definitions

(a) All capitalized terms not defined in this Addendum will have the meanings set forth in the Agreement.

(b) The following terms have the definitions given to them in the CCPA: "*Business*," "*Sale*," "*Service Provider*," and "*Third Party*."

(c) "*Controller*" means the entity that determines the purposes and means of the Processing of Personal Data. "Controller" includes a Business, Controller (as that term is defined in the GDPR), and equivalent terms in Data Protection Laws, as context requires.

(d) "*Data Exporter*" means the party that (1) has a corporate presence or other stable arrangement in a jurisdiction that requires an International Data Transfer Mechanism and (2) transfers Personal Data, or makes Personal Data available to, the Data Importer.

(e) "*Data Importer*" means the party that is (1) located in a jurisdiction that is not the same as the Data Exporter's jurisdiction and (2) receives Personal Data from the Data Exporter or is able to access Personal Data made available by the Data Exporter.

(f) "*Data Protection Law*" means any law applicable to Juspay or Merchant on the Processing of Personal Data, relating to data security, data protection, or privacy, and any implementing, derivative or related legislation, rule, regulation, and regulatory guidance, as amended, extended, repealed and replaced, or re-enacted.

(g) "*Data Subject*" means an identified or identifiable natural person.

(h) "*EEA*" means the European Economic Area.

(i) "*Personal Data*" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject. "Personal Data" includes Personal Information and Personal Data (as that term is defined in the GDPR), as context requires.

(j) "*Process*" or "*Processing*" means any operation or set of operations that a party performs on Personal Data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

(k) "*Processor*" means an entity that processes Personal Data on behalf of another entity. "Processor" includes Service Provider, Processor (as that term is defined in the GDPR), and equivalent terms in Data Protection Laws, as context requires.

(l) "*Security Incident*" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored, or otherwise processed by Juspay.

(m) "*Standard Contractual Clauses*" means the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021, available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

(n) "*Subprocessor*" means a Processor engaged by a party who is acting as a Processor.

Section 3 Description of the Parties' Personal Data Processing Activities and Statuses of the Parties

(a) Schedule 1 describes the purposes of the parties' Processing, the types or categories of Personal Data involved in the Processing, and the categories of Data Subjects affected by the Processing.

(b) Schedule 1 lists the parties' statuses under relevant Data Protection Law.

(c) The subject matter and duration of the Processing, the nature and purpose of the Processing, and the type of Personal Data and categories of Data Subjects may be more specifically described in a statement of work, Merchant purchase order, or written agreement signed by the parties' authorized representatives, which forms an integral part of the Agreement; if this is the case, the more specific description will control over Schedule 1.

Section 4 International Data Transfer

(a) Some jurisdictions require that an entity transferring Personal Data to a recipient in another jurisdiction take extra measures to ensure that the Personal Data has special protections if the law of the recipient's jurisdiction does not protect Personal Data in a manner equivalent to the transferring entity's jurisdiction (an "*International Data Transfer Mechanism*"). Controller shall notify the Processor if the parties need to comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law. Upon such notification by Controller, Processor reserves the right to terminate or suspend the services for such jurisdiction.

(b) If the International Data Transfer Mechanism on which the parties rely is invalidated or superseded, the parties will work together in good faith to find a suitable alternative.

(c) With respect to Personal Data of Data Subjects located in a jurisdiction that requires an International Data Transfer Mechanism, (e.g., the EEA, Switzerland, or the United Kingdom) that Merchant transfers to Juspay or permits Juspay to access, the parties agree that by executing this Agreement they also execute the Standard Contractual Clauses, which will be incorporated by reference and form an integral part of this Agreement. The parties agree that, with respect to the elements of the Standard Contractual Clauses that require the parties' input, Schedules 1 and 2 contain information relevant to the Standard Contractual Clauses' Annexes. The parties agree that, for Personal Data of Data Subjects in the United Kingdom, Switzerland, or another country specified in Schedule 1, they adopt the modifications to the Standard Contractual Clauses listed in Schedule 1 to adapt the Standard Contractual Clauses to local law, as applicable.

Section 5 Data Protection Generally

(a) Compliance. The parties will comply with their respective obligations under Data Protection Law and their privacy notices.

(b) For all processing of Personal Data under this Agreement, Merchant is Controller and Juspay is a processor.

(c) Cooperation

(1) Third-Party Requests. If Juspay receives any type of request or inquiry from a governmental,

legislative, judicial, law enforcement, or regulatory authority (e.g., the Federal Trade Commission, the Attorney General of a U.S. state, or a European data protection authority), or faces an actual or potential claim, inquiry, or complaint in connection with the parties' Processing of Personal Data (collectively, an "Inquiry"), Juspay will notify Merchant without undue delay unless such notification is prohibited by applicable law. Juspay will promptly provide Merchant with information relevant to the Inquiry, including any information relevant to the defense of a claim, to enable Merchant to respond to the Inquiry.

(2) Other Requirements of Data Protection Law. Upon request, Juspay will provide relevant information to Merchant to fulfill Merchant's obligations (if any) to conduct data protection impact assessments or prior consultations with data protection authorities, at Merchant's expense.

SECTION 6 Data Security and Confidentiality

(a) Confidentiality. Juspay will ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality obligations no less protective than those set forth in the Agreement or are under an appropriate statutory obligation of confidentiality.

(b) Security Controls. Juspay will abide by Schedule 2 and take all measures required in accordance with good industry practice and by Data Protection Law relating to data security (including pursuant to Article 32 of the GDPR).

SECTION 7 Juspay's Obligations as a Processor, Subprocessor, or Service Provider

(a) Juspay will have the obligations set forth in this Section 7 if it Processes the Personal Data of Data Subjects in its capacity as Merchant's Processor or Service Provider; for clarity, these obligations do not apply to Juspay in its capacity as a Controller, Business, or Third Party.

(b) Scope of Processing

(1) Juspay will Process Personal Data solely to provide Services to Merchant, carry out its obligations under the Agreement, and carry out Merchant's documented instructions. Juspay will not Process Personal Data for any other purpose, unless required by applicable law, and will not Sell Personal Data.

(2) Juspay will notify Merchant if it believes that it cannot follow Merchant's instructions or fulfill its obligations under the Agreement because of a legal obligation to which Juspay is subject, unless Juspay is prohibited by law from making such notification.

(c) Data Subjects' Requests to Exercise Rights. Juspay will promptly inform Merchant if Juspay receives a request from a Data Subject to exercise their rights with respect to their Personal Data under applicable Data Protection Law. Merchant will be responsible for responding to such requests. Juspay will not respond to such Data Subjects, unless instructed to by the Merchant. Juspay will provide Merchant with commercially reasonable assistance, upon request, to help Merchant to respond to a Data Subject's request, at Merchant's expense.

(d) Juspay's Subprocessors. Merchant provides general authorisation to Juspay's use of sub-processors to provide processing activities on Personal Data.

(e) **Security Incident**

(1) Without limiting Juspay's obligations under the Agreement with respect to Personal Data, on becoming aware of any Security Incident, Juspay will:

(i) notify Merchant without undue delay of the Security Incident;

(ii) promptly take all commercially reasonable steps to mitigate the effects of the Security Incident, or assist Merchant in doing so.

(2) Juspay will comply with this Section at Juspay's cost unless the Security Incident arose from

Merchant's negligent or willful acts or Juspay's compliance with Merchant's express written instructions.

(f) **Deletion and Return of Confidential Information**. At the expiration or termination of the the Addendum or upon request by Merchant or Merchant's Affiliate, Juspay will, without undue delay: (1) return all Personal Data (including copies thereof) to Merchant or the applicable Merchant Affiliate; or (2) upon request by Merchant or its Affiliate, destroy all Personal Data (including copies thereof), in each case unless the Law expressly requires otherwise or the parties otherwise expressly agree in writing. For any Merchant Confidential Information that Juspay retains after expiration or termination of the Agreement (for example, because Juspay is legally required to retain the information), Juspay will continue to comply with the data security and privacy provisions in this Addendum and Juspay must De-identify or aggregate Personal Data (if any) to the extent feasible.

[Remainder of this page is intentionally left blank]

Schedule 1: Description of the Processing and Subprocessors

Processing Activity	Status of the Parties	Categories of Personal Data that May Be Processed *The categories listed are descriptive and do not necessarily mean that the parties are processing each category of data listed.*	Categories of Sensitive Data that May Be Processed *The categories listed are descriptive and do not necessarily mean that the parties are processing each category of data listed.*	Applicable SCCs Module
Juspay Processes Personal Data to provide the Services.	Merchant is the Controller. Juspay is the Processor.	● End user contact information (Mobile number, Email, Address) ● Payment information (Credit/ Debit card number, Bank account number) ● Transaction data (Transaction history of customer including transaction identifiers, merchant order ID, refund history)	● None	Module 2 Module 3, if Merchant acts as a Processor to another Controller

Subprocessors

Juspay uses AWS as Subprocessors for cloud infrastructure service.

Information for International Transfers

Frequency of Transfer

Continuous for all Personal Data.

Retention Periods

As Controllers, the parties retain Personal Data for as long as they have a business purpose for it or for the longest time allowable by applicable law.

As a Processor, Juspay retains Personal Data it collects or receives from Merchant for the duration of the Agreement and consistent with its obligations in this DPA.

For the purpose of the Standard Contractual Clauses:

- Clause 7: The parties do not adopt the optional docking clause.
- Clause 9, Module 2(a), if applicable: The parties select Option 2. The time period is 30 days.
- Clause 9, Module 3(a), if applicable: The parties select Option 2. The time period is 30 days.
- Clause 11(a): The parties do not select the independent dispute resolution option.
- Clause 17: The parties select Option 1. The parties agree that the governing jurisdiction is Ireland.
- Clause 18: The parties agree that the forum is Member State.

- Annex I(A): The data exporter is the Data Exporter (defined above) and the data importer is the Data Importer (defined above).
- Annex I(B): The parties agree that Schedule 1 describes the transfer.
- Annex I(C): The competent supervisory authority is the Irish Data Protection Commission.
- Annex II: The parties agree that Schedule 2 describes the technical and organizational measures applicable to the transfer.

For the purpose of localizing the Standard Contractual Clauses:

- Switzerland
  - The parties adopt the GDPR standard for all data transfers.
  - Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), are the Federal Data Protection and Information Commissioner and, concurrently, the EEA member state authority identified above.
  - Clause 17: The parties agree that the governing jurisdiction is Switzerland.
  - Clause 18: The parties agree that the forum is Switzerland. The parties agree to interpret the Standard Contractual Clauses so that Data Subjects in Switzerland are able to sue for their rights in Switzerland in accordance with Clause 18(c).
  - The parties agree to interpret the Standard Contractual Clauses so that "Data Subjects" includes information about Swiss legal entities until the revised Federal Act on Data Protection becomes operative.
- United Kingdom
  - The parties agree that the Standard Contractual Clauses are deemed amended to the extent necessary that they operate for transfers from the United Kingdom to a Third Country and provide appropriate safeguards for transfers according to Article 46 of the United Kingdom General Data Protection Regulation ("*UK GDPR*"). Such amendments include changing references to the GDPR to the UK GDPR and changing references to EU Member States to the United Kingdom.
  - Clause 17: The parties agree that the governing jurisdiction is the United Kingdom.
  - Clause 18: The parties agree that the forum is the courts of England and Wales. The parties agree that Data Subjects may bring legal proceedings against either party in the courts of any country in the United Kingdom.

Schedule 2: Technical and Organizational Security Measures

Service Infrastructure Management

Physical Security: Juspay has a security program that manages visitors, office entrances, and information assets across geographically distributed offices.

Network Security: Juspay has established procedural and technical standards for deploying network functions to production. These standards include baseline configurations for network components, network architecture, and approved protocols and ports. All network components are monitored to prevent malicious activities that might affect the company's infrastructure and to maintain their compliance with technical standards. Using a virtual private network (VPN) and the trusted firewalls, Juspay keeps the service environment safe and secure from external threats and vulnerabilities.

Monitoring: Juspay's monitoring program focuses on detecting and reporting vulnerabilities in our service and products. All system changes and vulnerabilities are monitored and audited. Based on inbound security reports, our engineers quickly analyze vulnerabilities, find the best solutions, and resolve issues.

Audit Log: Juspay only grants authorized employees' access to customer data based on the principle of least-privilege. They are required to use monitoring tools to detect intrusion attempts and other security-related alerts and to record audit logs for their activities. Audit logs are maintained for all operations and activities such as privileged user access and unauthorized access attempts of customer data.

Access Security

Authentication - MFA, OTP: Access to customer data is restricted to authorized employees. Juspay applies multi-factor authentication (MFA) and controls for administrative access to its system. For secure authentication, employees are required to use a proprietary VPN solution with MFA when accessing the system. And upon a data owner's request and approval, temporary access to customer data is granted to only a limited group of employees. All related activities are tracked by audit logs. Access to the company's system and customer data requires two-factor authentication according to the following criteria: a unique user ID, strong password, OTP, and/or certificate.

Password Management: Employees are required to change passwords regularly according to Juspay's internal policy. The corporate password requirements include complexity, length, history, and duration.

Endpoint Management: Juspay monitors, manages, and restricts all workstations and mobile devices that are used to access the company's system. All workers - regular employees and independent contractors - must install an endpoint protection agent that consists of antimalware, intrusion prevention, and a firewall. Endpoint protection has an administrative console that allows Juspay to monitor any employee's access and events within the Juspay system environment.

Change Management

Development: In the event of software releases, the company uses a proprietary ticketing system to document procedures for tracking, testing, approving, and validating. A change management project is created when the ticketing system tracks activities from software development and customer requests.

Tracking: All audit logs are recorded for easy tracking of the changes in the ticketing system. Juspay regularly checks these logs to make sure procedures comply with system change management. Juspay also maintains updates to management policies regarding security code reviews and emergency fixes.

Vulnerability Management: Juspay operates its own vulnerability management program that actively investigates for security vulnerabilities using a combination of automated scans and penetration tests. Automated scans identify all types of vulnerabilities in the software, system, and network components. Once vulnerabilities are identified, the vulnerability management program classifies and remediates vulnerabilities across all Juspay services. Juspay also takes corrective actions when necessary, based on the results of our annual penetration tests conducted by an external independent third-party.

Customer Data Security

Incident Management: Juspay has established protocols and guidelines for responding to emergency security incidents. All incidents are thoroughly investigated, documented, and reported to our Incident Response team for timely mitigation, including suspected or known violations of privacy and security.

Retention: The contract and service licensing agreement signed between Juspay and a client sets out the duration of how long Juspay retains customer data after the termination of contract. Customer data will be removed from the Juspay server accordingly.

Business Continuity

Business Continuity Plan: Business Continuity Planning (BCP) has been established for Juspay services, which provides detailed procedures for recovery and reconstitution of systems known as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Our BCP is reviewed on an annual basis.

Disaster Recovery Drills: The engineering department conducts annual business continuity and disaster recovery drills to test communication plans, fail-over scenarios, operational transition, and other emergency responses. All teams that participate in the business continuity and disaster recovery exercise develop drill plans and post-mortems.