DATA PROTECTION ADDENDUM

This Data Processing Addendum ("**DPA**" or "**Addendum**") forms part of the agreement for services between ("**Planet**") and (the "**Merchant**") dated (the "**Agreement**").

Planet and the Merchant (each individually referred to as a "**Party**", and jointly as the "**Parties**") agree that this DPA states the data protection requirements that apply to the processing of Personal Data (or Shared Personal Data, as applicable) by the Parties for the purposes set out in the Agreement and/or this DPA.

1. Definitions

The following definitions apply in this Addendum:

1.1. **Affiliates**: any individual, corporation, partnership, association or business that directly or indirectly through one or more intermediaries, controls, or is controlled by or is under common control of a party as applicable, or their respective successors. The term "control" including the terms "controlling," "controlled by," and "under common control with" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a corporation, partnership, association or business, whether through the ownership of voting shares, by contract or otherwise. Affiliates shall include such entities whether now existing or later established by investment, merger or otherwise, including the successors and assigns of such entities.

1.2. **Applicable Laws**: any and all laws, regulations, government mandated decisions, terms, guidance and any modification thereof, which has relevant standing in the relevant jurisdiction, as well as any decision made by relevant and competent government entities, in all relevant jurisdictions to the Agreement and including but not limited to regulations governing the banking intermediary profession and any Monetary and Financial codes applicable in relevant countries, legislation on anti-money laundering (AML), counter terrorist financing (CTF), embargos, sanctions, bribery, misconduct, confidential information (including intellectual property and trade secrets), behaviour of financial institutions and Data Protection Laws.

1.3. **Data Controller**: has the meaning given to the term 'controller' where it determines the purposes of any personal data and the means of processing it as set out in Data Protection Laws.

1.4. **Data Processor**: has the meaning given to the term 'processor' where any other body who processes personal data on behalf of a data controller as set out in Data Protection Laws.

1.5. **Data Protection Laws**: the General Data Protection Regulation 2016/679 (GDPR), the New Swiss Federal Act on Data Protection (nFADP), the UK Data Protection Act 2018, the UK Privacy and Electronic Communications Regulations 2003, the French law n°78-17 of 6 January 1978 on information technology, files and freedoms, and all other Applicable Laws, relating to the processing of Personal Data, each as may be amended or superseded from time to time.

1.6. **Data Security Incident**: means any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the Personal Data (or the Shared Personal Data, as applicable) and/or any breach of the security and/or confidentiality leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data (or the Shared Personal Data, as applicable).

1.7. **Data Subject**: an identified or identifiable natural person to which Personal Data relates.

1.8. **Data Subject Request:** means a formal request made by a Data Subject with the aim of exercising their rights (i) to access its Personal Data; (ii) have its Personal Data corrected or erased; (iii) to restrict or object to processing of its Personal Data; (iv) to request the portability of its Personal Data; (v) not to be subject of automated decision making (including profiling); or, (vi) in relation to any other right that Data Subject are entitled to exercise in any relevant jurisdiction to which this DPA applies.

1.9. **Personal Data**: any personal data that identifies an individual person (as set out in Data Protection Laws) which is processed in connection with the Agreement.

1.10. **Shared Personal Data**: any personal data that identifies an individual person (as set out in Data Protection Laws) which is processed in connection with the Agreement if the Parties act as independent data controller in the context of a "Data Controller-to-Data Controller relationship".

1.11. **Standard Contractual Clauses**: mean the (i) the standard contractual clauses for international transfers published by the European Commission on June 4, 2021 governing the transfer of Personal Data from the EEA to third countries as adopted by the European Commission (available on European Commission website: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en), and the Swiss Federal Data Protection and Information Commissioner ("**Swiss FDPIC**") relating to data transfers to third countries (collectively "**EU SCCs**"); (ii) the international data transfer addendum ("**UK Transfer Addendum**") adopted by the UK Information Commissioner's Office ("**UK ICO**") for data transfers from the UK to third countries; (iii) any similar such clauses (as applicable) adopted by a data protection regulator relating to data transfers to third countries; or (iv) any successor clauses to (i) – (iii).

1.12. **Sub-processor**: means an entity a Processor engages to process Personal Data on that Processor's behalf.

1.13. **Supervisory Authority**: means an independent public authority which is either: (i) established by an EU member state pursuant to Article 51 of the GDPR; or, (ii) the public authority governing data protection that has supervisory authority and jurisdiction over you.

2. Data protection roles

In the course of Planet providing the Services to the Merchant under the Agreement, the Parties may from time-to-time provide or make available Personal Data to the other Party. The Parties agree that depending on the Services contracted, the data protection roles assigned to them for the purposes of Data Protection Laws will either be: (i) independent Data Controllers (in the context of a Data Controller-to-Data Controller relationship); (ii) Data Controller (in the context of a Data Processor-to-Data Controller relationship); or, (iii) Data Processor on behalf of the other Party (in the context of a Data Processor-to-Data Controller relationship). Considering this:

a) **If the Parties are processing Personal Data acting as independent Data Controllers, Paragraph 3 of this DPA shall apply.**
b) **If a Party is processing Personal Data acting as a Data Controller, in the context of a Data Controller-to-Data Processor relationship, Paragraph 4 of this DPA shall apply to such Party.**
c) **If a Party is processing Personal Data acting as a Data Processor, on behalf of the other Party, Paragraph 5 of this DPA shall apply to such Party.**

A full description of the roles and purposes for which Personal Data (or Shared Personal Data, as applicable) is processed in the context of the services under the Agreement is included in Appendix 1.

3. Obligations applicable to the Parties acting as independent Data Controllers

This Paragraph 3 shall apply in the event of the Parties acting as independent Data Controllers.

3.1. General

3.1.1. The Parties shall regularly disclose to each other Personal Data for the purposes set out in the Agreement and/or the DPA ("**Shared Personal Data**") and agree that in relation to such Shared Personal Data, each Party acts as a Data Controller in its own right and shall independently determine the purposes and means of such data processing.

3.2. Processing of Shared Personal Data

3.2.1. Where a Party act as a Data Controller of the Shared Personal Data in respect of Services, it shall be responsible for complying with and performing its obligations under Data Protection Laws and in particular for:

a) making sure that the Shared Personal Data provided or made available under the Agreement is accurate and up to date;
b) ensuring that it has an appropriate legal basis for the processing of the Shared Personal Data as described in this DPA and/or the Agreement;
c) making sure that all necessary fair processing notices (commonly known as "privacy notices" or "privacy policies") are provided to Data Subjects concerned by the data processing at the time of collecting their Personal Data to enable the lawful processing (including the collection and sharing) of the Shared Personal Data for the purposes set out in the Agreement and/or the DPA;

d) making sure that unless another legal basis set forth in Data Protection Laws supports the lawfulness of the processing, that any necessary Data Subject consents to the processing are obtained and recorded, and in the event a consent is revoked by a Data Subject, ensuring that it is communicated to the other Party.

3.2.2. Each Party undertakes not to provide to the other Party any special category of Personal Data (such as health data) that is not required for performance of the Services.

3.3. Data Security

3.3.1. Each Party shall take reasonable steps to ensure the reliability of individuals who may process Shared Personal Data including ensuring: (i) that access is strictly limited to those individuals who need to know or access the relevant Shared Personal Data for the purposes described in the Agreement and/or this DPA; and, (ii) that such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3.3.2. The Parties shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk (taking into account the nature, scope, context and purposes of processing), including from unauthorised or unlawful processing, or accidental loss or destruction of, or damage to such Shared Personal Data. In particular, Planet will apply the following Technical and Organisational Measures located at https://www.weareplanet.com/technical-and-organisational-measures, a summary of which can be found in Appendix 2.

3.3.3. The Party receiving the Shared Personal Data shall not retain or process it for longer than is necessary for the purposes set out in the Agreement and/or this DPA and shall be responsible for implementing appropriate measures to ensure the Shared Personal Data is destroyed or deleted when it is not necessary for such purposes. Notwithstanding the previous, each Party may continue to retain the Shared Personal Data in accordance with any applicable statutory or professional retention periods.

3.4. Data Subject Rights

3.4.1. Each Party shall be responsible for dealing with its own Data Subject Requests in relation to the Shared Personal Data and shall provide assistance as reasonably required to enable the other Party to comply with such Data Subject Requests.

3.4.2. If a Party receives a Data Subject Request in relation to the Shared Personal Data that concerns processing in respect of which the other Party is the Data Controller, the Party receiving such Data Subject Request shall promptly forward it to the other Party. Upon reasonable written request, the Party receiving the Data Subject Request shall provide with reasonable cooperation and assistance to enable the other Party to comply with such Data Subject Request and meet applicable timescale set out under Data Protection Laws.

3.5. Data Security Incidents

3.5.1. When a Party becomes aware of a Data Security Incident that has a material impact on the processing of the Shared Personal Data, it shall promptly notify and cooperate with the other Party in order to enable it to perform an investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the Data Security Incident.

3.5.2. Each Party, in the event that a Data Security Incident relating to the Shared Personal Data occurs, or under a suspicion that a Data Security Incident event has occurred or may occur, will inform the other Party in writing as soon as possible with all relevant information concerning the event details in order to allow such Party to comply with Data Protection Laws. The relevant information of the Data Security Incident will include:

a) name, trading name and the information alleged to have been affected by it;
b) a description of its nature, including where possible the categories and approximate number of Data Subjects concerned;
c) the name and contact details of the data protection officer or another contact point where more information can be obtained;
d) a description of its likely consequences;
e) a description of the measures taken or proposed to be taken to address it including, where appropriate, measures to mitigate its possible adverse effects; and,
f) a copy of all correspondence relating to it, including any correspondence with any Data Subjects.

3.6. Mutual assistance

3.6.1. Each Party shall, on reasonable request, provide the other Party with reasonable assistance, information and cooperation to ensure compliance with their respective obligations under Data Protection Laws.

3.6.2. If a Party receives any complaint, notice or communication from a Supervisory Authority which relates directly to the other Party data processing of the Shared Personal Data, or a potential failure by such Party to comply with Data Protection Laws in respect of the Services, the Party receiving the complaint, notice or communication shall, to the extent permitted by Applicable Laws, promptly notify the other Party and provide such information as it shall reasonably request in that regard.

3.7. International Data Transfers

3.7.1. The Parties may only process Shared Personal Data within the EEA, the UK, or Switzerland (as applicable) or in other countries recognised by the European Commission, the ICO or the Swiss FDPIC (as applicable), as ensuring an adequate level of protection of personal data with regard to data privacy and the fundamental rights and freedoms of individuals.

3.7.2. Where a Party transfers or exports Shared Personal Data to a third country outside the EEA, the UK, or Switzerland (as applicable) without an adequate level of protection as declared by the European Commission, the ICO or the Swiss FDPIC (as applicable) it shall comply with its obligations under Data Protection Laws by: (i) using any reasonable transfer control mechanisms recognised by Data Protection Laws as an appropriate safeguard; or, (ii) by governing the terms of such transfer by the Standard Contractual Clauses, which shall be incorporated to this Agreement.

3.7.3. Furthermore, the Party transferring or exporting the Shared Personal Data shall implement and incorporate to this DPA the adequate supplementary measures which are pertinent in accordance with the regulatory risk of the country of destination, ensuring an essentially equivalent level of protection for data as in the EEA, the UK or Switzerland, as applicable.

3.7.4. To the extent the Party transferring or exporting the Shared Personal Data is relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Parties agree to cooperate in good faith to pursue a suitable alternate mechanism that can lawfully support the transfer.

4. Obligations applicable to a Party acting as Data Controller

This Paragraph 4 shall apply in the event of a Party acting as Data Controller in the context of a Data Controller-to-Data Processor relationship.

4.1. General

4.1.1. Where a Party act as Data Controller, and the other Party holds the role of Data Processor, the former shall have the sole and exclusive authority to determine the purposes and means of processing Personal Data received from or through the other Party, and shall be responsible for complying with and performing its obligation under Data Protection Laws and in particular for:

a) making sure that any Personal Data provided or made available under the Agreement is accurate and up to date;
b) providing only instructions relating to the processing of Personal Data that are lawful;
c) ensuring that it has an appropriate legal basis for the processing of Personal Data as described in this DPA and/or the Agreement;
d) making sure that all necessary fair processing notices (commonly known as “privacy notices” or “privacy policies”) are provided to Data Subjects concerned by the data processing at the time of collecting their Personal Data to enable the lawful processing (including the collection and sharing) of the Personal Data for the purposes set out in the Agreement and/or the DPA;
e) making sure that unless another legal basis set forth in Data Protection Laws supports the lawfulness of the processing, that any necessary Data Subject consents to the processing are obtained and recorded, and in the event a consent is revoked by a data subject, ensuring that it is communicated to Data Processor; and,
f) implementing and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk (taking into account the nature, scope, context and purposes of processing), including from unauthorised or unlawful processing, or accidental loss or destruction of, or damage to such Personal Data.

4.1.2. The Data Controller undertakes not to provide to the Data Processor any special category of Personal Data (such as health data) that is not required for performance of the Services.

5. Obligations applicable to a Party acting as Data Processor

This Paragraph 5 shall apply in the event of a Party acting as Data Processor on behalf of the other Party. For this purpose, where a Party processes Personal Data behalf of the other Party, it shall comply with its obligations under Data Protection Laws which applies in jurisdictions where it conducts business, and with the obligations assumed by this DPA as follows:

5.1. Data Security

5.1.1. The Data Processor will:

a) comply with the data security standards communicated by and/or agreed with the other Party;
b) retain all Personal Data in a secure environment to make sure that Personal Data is not disclosed to a third party (other than as permitted under the Agreement) or misused by a third party;
c) take reasonable measures in view of the nature and risks presented by the data processing, to make sure that a Data Security Incident does not occur; and,
d) not circumvent any technology used by us or other third parties to protect content accessible via the Services.

5.1.2. The Party acting as Data Processor undertakes to implement all appropriate technical and organizational measures to protect Personal Data, taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the data processing as well as the risks, degree of probability and severity, to the rights and freedoms of Data Subjects, in order to guarantee a level of security appropriate to the risk. In particular:

a) Where the Merchant acts as Data Processor shall be required to take all appropriate technical and organisational measures, including but not limited to the measures set out in Appendix 3 to ensure an appropriate level of security for the Personal Data (including to protect it against accidental or unlawful destruction, loss or alteration, and against unauthorised disclosure or access).
b) Where Planet acts as Data Processor will apply the following Technical and Organisational Measures located at https://www.weareplanet.com/technical-and-organisational-measures, a summary table of which can be found in Appendix 2.

5.1.3. Without limiting the material nature of any other Personal Data disclosures, a breach of this Paragraph 5.1. shall be considered a material breach of the Agreement.

5.2. Confidentiality and secrecy

5.2.1. The Data Processor undertakes to maintain its confidentiality duty with respect to the Personal Data to which it has accessed as a result of this Agreement. For this purpose, the Data Processor will make sure that persons authorised to process the Personal Data have undertaken to respect confidentiality or are subject to statutory confidentiality obligations and that all of their respective employees are trained in line with their respective responsibilities under Data Protection Laws.

5.3. Instructions from the Data Controller

5.3.1. The Data Processor will process the Personal Data only on written instructions from the Data Controller (including as documented in this DPA) in connection with the Services provided under the Agreement and must not be used for any purpose other than those specified in this DPA and/or the Agreement. The Data Processor undertakes to inform the Data Controller as soon as possible in writing in the event of the former considering that any instruction from the Data Controller may breach Data Protection Laws.

5.4. Subcontracting

5.4.1. The Data Processor is authorized to use sub-processors for carrying out activities part of this Agreement. Notwithstanding this, if after the date of this Addendum new sub-processors are engaged by the Data Processor, the Data Controller may reasonably object to a change or use of a new sub-processor on legitimate grounds by notifying the Data Processor in writing within ten (10) days after notice of a new sub-processor has been provided. If there has been no objection, the sub-processor shall be deemed to have been accepted.

5.4.2. In particular, the Merchant acknowledges that Planet's sub-processors are essential to provide the Services and that if it objects to Planet's use of a sub-processor, then notwithstanding anything to the contrary in the Agreement (including this Addendum), Planet will not be obligated to provide the Merchant with the Service for which Planet uses that sub-processor.

5.4.3. Planet's and Merchant's sub-processors are listed in Appendix 4 and, by signing this Addendum, Planet and the Merchant are respectively authorising the other Party to use these sub-processors.

5.4.4. The Data Processor shall enter into an agreement in writing with its sub-processors imposing obligations that are consistent with those in this Addendum and/or the Agreement. If a sub-processor fails to fulfil its data protection obligations under that agreement, the Data Processor shall be liable to the Data Controller for the acts and omissions of its sub-processor to the same extent the Data Processor would be liable if performing the relevant Service directly under the Agreement.

5.4.5. The Data Processor shall agree a third-party beneficiary clause with sub-processor whereby, in the event that the Data Processor has factually disappeared, ceased to exist in law or has become insolvent, the Data Controller shall have the right to terminate the sub-processor agreement and to instruct sub-processor to erase or return the personal data.

5.5. Assistance to Data Controller, Compliance and Audits

5.5.1. By applying appropriate technical and organisational measures and insofar as it is possible, the Data Processor shall assist the Data Controller with Data Subject Requests it may receive. The Data Controller will have the right to instruct the Data Processor in writing to cease to respond to such Data Subject Requests at any time. When the Data Processor receives a Data Subject Request it will respond to such Data Subject Request in compliance with applicable Data Protection Laws. The Data Controller acknowledges that the handling of such Data Subject Requests by the Data Processor on behalf of the Data Controller does not imply any exemption or waiver from the legal obligations imposed by the applicable Data Protection Laws.

5.5.2. The Data Processor, taking into account the nature of processing and the information it has available, shall also assist the Data Controller in ensuring compliance with obligations pursuant Data Protection Laws that are relevant to the data processing covered by this DPA, including notifications to a Supervisory Authority or to Data Subjects, the process of undertaking a Data Protection Impact Assessment, and with prior consultations with Supervisory Authorities.

5.5.3. The Data Processor will make available to the Data Controller all information necessary to demonstrate compliance with its respective obligations set out in this Addendum and allow for and contribute to data audits, including inspections, if the Data Controller so requires.

5.5.4. The Data Controller may carry out, at its own expense, once a year, with no less than 30 days' notice, any audit to confirm compliance with Data Protection Laws. The audit shall be carried out either by any of the Parties' personnel, or by an independent entity, chosen by the auditing party, with independent members having the required professional qualifications, bound by an obligation of confidentiality, and not belonging to a company which is directly competing with any of the Parties in respect of the Services. The Parties agree that:

a) the audit shall not include financial or personal data not directly and solely related to each of the Parties, any information which could affect each of the Parties' security systems and data (i.e., risk to the confidentiality of information), and the source code of computer programs used in the performance of the Services;
b) the auditor shall not copy any document, file, data or information, in whole or in part, take photographs, scan, make any audio/video or computer files / programs without prior consent; and
c) the audit must take place during business hours and be conducted in a manner that does not disrupt the audited Party's operations or services.

5.6. International Data Transfers

5.6.1. The Data Processor may process Personal Data within the EEA, the UK, or Switzerland (as applicable) or in other countries recognised by the European Commission, the ICO or the Swiss FDPIC (as applicable) as ensuring an adequate level of protection of Personal Data regarding data privacy and the fundamental rights and freedoms of Data Subjects.

5.6.2. Where the Data Processor transfers or exports Personal Data to a third country outside of the EEA, the UK, or Switzerland (as applicable) without an adequate level of protection as declared by the European Commission, the ICO

or the Swiss FDPIC (as applicable), the Data Processor shall comply with its obligations under Data Protection Laws by: (i) using any reasonable transfer control mechanisms recognised by Data Protection Laws as an appropriate safeguard; or, (ii) by governing the terms of this transfer by the Standard Contractual Clauses, which shall be incorporated to this DPA.

5.6.3. Furthermore, the Data Processor shall implement and incorporate to this DPA the adequate supplementary measures which are pertinent in accordance with the regulatory risk of the country of destination, ensuring an essentially equivalent level of protection for data as in the EEA, the UK, or Switzerland, as applicable.

5.6.4. To the extent the Data Processor is relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Parties agree to cooperate in good faith to pursue a suitable alternate mechanism that can lawfully support the transfer.

5.7. Data Security Incidents

5.7.1. When the Data Processor becomes aware of a Data Security Incident that has a material impact on the processing of the Personal Data that is the subject of the Agreement, it shall promptly notify the Data Controller about it, shall at all times cooperate with the Data Controller, and shall follow the Data Controller's instructions with regard to such Data Security Incident, in order to enable the Data Controller to perform an investigation, to formulate a correct response, and to take suitable further steps in respect of it.

5.7.2. The Data Processor, in the event that a Data Security Incident occurs, or under a suspicion that a Data Security Incident event has occurred or may occur, will inform the Data Controller in writing as soon as possible with all relevant information concerning the event details in order to assist the Data Controller to comply with Data Protection Laws. The relevant information of the Data Security Incident will include:

a) name, trading name and the information alleged to have been affected by it;
b) a description of its nature, including where possible the categories and approximate number of Data Subjects concerned;
c) the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;
d) a description of its likely consequences;
e) a description of the measures taken or proposed to be taken by the Data Processor to address it including, where appropriate, measures to mitigate its possible adverse effects; and,
f) a copy of all correspondence relating to it including any correspondence with any Data Subjects.

5.8. Record of processing

5.8.1. The Data Processor will keep a written record of all categories of data processing activities performed on behalf of the Data Controller when acting as the Data Processor including:

a) the name and contact details of the Data Controller on whose behalf it is acting, any subsequent sub-processors and, where applicable, the data protection officer;
b) the categories of data processing activities carried out on behalf of the Data Controller or the Data Subject;
c) where applicable, the transfers of Personal Data to a third country or to an international organisation, including the identification of this third country or international organisation and, in the case of the transfers referred to in Data Protection Laws;
d) to the extent possible, a general description of the technical and organisational security measures.

5.9. Return or destruction of Personal Data

5.9.1. After the contracted Service has been performed or upon termination of the Agreement, the Data Processor shall return and/or destroy, at the Data Controller's discretion, and in the manner and timelines indicated by the Data Controller, all Personal Data to which it has gained access during the contractual relationship and any other document considered confidential unless any legal requirement or impediment requires otherwise.

5.9.2. Notwithstanding the previous, if no such instruction is received from the Data Controller within 3 months after the performance of the Services or termination of the Agreement, the Personal Data will be destroyed. The Data Controller

may ask the Data Processor to provide a written certificate of destruction of the Personal Data and documents destroyed.

5.9.3. Subject to the acceptance by the Data Controller of a fee quote, the Data Processor will provide the Personal Data to the Data Controller or any third party designated by the Data Controller, in a standard market format, in order to continue the processing of the Personal Data.

6. Miscellaneous

6.1. The Addendum constitutes the entire agreement between Planet and the Merchant regarding its subject matter and it supersedes any earlier agreements that the Parties may have had regarding the subject matter.

6.2. Except as specifically modified or amended by the terms of this Addendum, the Agreement and all provisions contained therein or the terms of any other agreement or document referred to therein are, and shall continue, in full force and effect.

6.3. Should the terms of this Addendum conflict with the terms of any other amendment or addendum and/or the Agreement regarding Personal Data processing, then the terms of this Addendum shall prevail.

6.4. The governing law and jurisdiction in respect of this Addendum shall be in accordance with the governing law and jurisdiction in the Agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be duly executed and delivered by their proper and duly authorised officers as of the day and year first above written.

Planet	**Merchant**
By:_____	By:_____
Name:	Name:
Title:	Title:

APPENDIX 1

Purposes of processing

The Parties understand that Planet may use Personal Data (or Shared Personal Data, as applicable) on behalf of the Data Subject for:

a) Performing its obligations under the Agreement (e.g., to allow the management of transactions);
b) Complying with its obligations under Applicable Laws and with Supervisory Authorities requirements and requests (e.g., to verify the identity of the Data Subjects);
c) Its legitimate interests (e.g., to improve our engagement feedback for services provided);

The Parties undertake that Personal Data (or Shared Personal Data, as applicable) will never be sold or provided to third parties without prior written authorisation of the Data Subjects concerned.

Data Protection Roles

Service	Planet	Merchant	Data Category and Personal Data usually processed
Gateway	Processor	Controller	Data of Merchant's customer availing of the Services including: PAN, CVV, expiry date and post code where required for verification purposes. For APM, only account number processed.
PCI Proxy	Processor	Controller	Data of Merchant's customer availing of the Services including: PAN, card expiry date, CVV.
Acquiring	Controller	Controller	Data of Merchant's customer availing of the Services including: PAN, CVV, expiry date and post code where required for verification purposes. For APM, only account number processed.
Equipment Rental	Processor	Controller	Certain limited data of Merchant's customer availing of the Services related to the payment transaction carried out through the equipment including amount of the transactions and authorisation code.
Equipment Purchase	Processor	Controller	Certain limited data of Merchant's customer availing of the Services related to the payment transaction carried out through the equipment including amount of the transactions and authorisation code (if applicable).
Currency Conversion	Processor	Controller	Data of Merchant's customer availing of the Services including: IP Address (only for DCC), Card BIN (first 6 digits), tokenized card data, device information.
VAT Refunding	Controller	Processor	Data of Merchant's customer availing of the Services: including PAN, CVV, expiry date and post code where required for verification purposes. For APM, only account number processed.
Gift Card Solution Software	Processor	Controller	Data of Merchant's customer availing of the Services: name, email address and postal address (if physical gift card is issued).
Retail Software	Processor	Controller	Data of Merchant's customer availing of the Services including: name, email address, phone number, postal address; User login information (IP address, browser type); User's billing information (contact information, last four digits of the credit card and type of payment method).
All Services, as applicable	Processor	Controller	Data for Merchant's personnel, including: names, work email addresses, phone number, job roles for uploading into the training platform for the purpose of arranging and managing training services requested by Merchant

APPENDIX 2

Where Planet process Personal Data (or Shared Personal Data, as applicable) will apply the following Technical and Organisational Measures located at https://www.weareplanet.com/technical-and-organisational-measures, a summary table of which is included as follows:

Category	Subcategory	Measure
Security Programmes and Policies	Security Programme	Planet maintains and enforces a security programme that governs how Planet manages security.
	Privacy Programme	Planet maintains and enforces a privacy programme that governs how Personal Data is collected, used, and shared.
Risk and Asset Management	Risk Assessments	Planet proactively manages risk through our Enterprise Risk Management Framework and robust Three Lines Model.
	Asset Management	Planet maintains and enforces an asset management programme that appropriately classifies and controls hardware and software assets throughout their life cycle.
Personnel Education and Controls	Acknowledgement of Responsibility	All Planet employees, and independent contractors who may have access to data, including those who process Personal Data, acknowledge their data security and privacy responsibilities under Planet's policies.
Training and Awareness	Annual Security and Privacy Training	Planet's employees complete annual awareness training on GDPR, KYC, AML, and Information Security.
Network and Operations Management	Policies and Procedures	Planet 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	Planet performs periodic vulnerability assessments and penetration testing on its systems and applications, including those that process Personal Data.
Technical Access Controls	Access Control	Planet implements measures to prevent data processing systems from being used by unauthorised persons.
	Data Access Control	Planet 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 authorisation.
Physical Access Controls	Data Centre Security	Planet leverages trusted third-party service providers for hosting its production infrastructure. Planet depends on these third parties to oversee the physical access controls to the data centre facilities under their management.
	Office Security	Physical access to Planet offices is controlled using mechanisms such as guest sign-in, electronic door locks, alarm systems, and secure storage rooms.
	Third-Party Audits	Planet reviews third-party audit reports to verify that Planet's service providers maintain appropriate physical access controls for our managed data centres.
Availability Controls	Availability	Planet has in place measures to guarantee the prompt restoration of the availability and access to Personal Data in the event of a physical or technical incident.

Category	Subcategory	Measure
Disclosure Controls	Disclosure	Planet implements measures to ensure that Personal Data cannot be read, copied, modified, or deleted without authorisation during electronic transmission, transport, or storage on storage media (manual or electronic).
Separation Controls	Separation	Planet implements measures to ensure that Personal Data collected for different purposes can be processed separately.
Certifications	PCI Compliance	Planet commits to delivering its services in accordance with PCI-DSS compliance standards, as applicable to our offerings.
Encryption	Encryption Mechanisms	Planet employs data encryption mechanisms at various stages to reduce the risk of unauthorised access to data while at rest and during transit. Furthermore, access to Planet's cryptographic key materials is limited to a select group of authorised Planet personnel.
Data Security Incident Management and Notification	Incident Management	Planet implements a data security incident management programme that governs how Planet manages incidents.
Data Retention and Deletion	Data Retention	Planet implements and maintains data retention policies and procedures related to Personal Data and reviews these policies and procedures as appropriate.

APPENDIX 3

Where Planet act as the Data Controller and the Merchant as Data Processor, the Merchant is required to implement the following technical and organisational measures to ensure a level of security commensurate to the risk, including, inter alia as appropriate:

1. Setting the functions and responsibilities of personnel who process Personal Data and informing personnel of their functions and responsibilities when it comes to observing Data Protection Laws and regulations;
2. Defining roles and profiles for users of the applications and systems through which the Personal Data is processed, in accordance with the established functions and responsibilities, so as to prevent any unauthorized access to Personal Data or resources. This access control system must guarantee appropriate user identification and authentication mechanisms, such as passwords that must be reset periodically, biometric data, multi-factor authentication, automatic automatic blocking of the user following a set number of unsuccessful login attempts;
3. Applying measures that allow the pseudonymization and encryption of Personal Data;
4. Putting into effect records of control and access to files and media containing Personal Data which must also feature mechanisms to restrict access;
5. Applying automated measures that restrict that access for unauthorized users or where the relevant storage period has expired, such as through erasure techniques and data pseudonymization;
6. Implementing procedures to limit physical access to the facilities at which the information systems or physical media are located;
7. Applying measures to ensure the continued confidentiality, integrity, availability, and resilience of systems and services;
8. Implementing procedures for recovering Personal Data if it is destroyed lost or altered under the supervision and subject to the approval of the data protection officer;
9. Implementing procedures to detect, assess and if necessary report any Data Security Incidents that might affect the rights and freedom of Data Subjects;
10. Conducting periodic compliance reviews and defining and executing action plans to mitigate the risks detected;
11. Applying any other appropriate technical and organisational measures to ensure a level of security commensurate to the risk.

APPENDIX 4

Planet's sub-processors are available for consultation at: https://www.weareplanet.com/legal/subprocessor-and-service-provider-list

Merchant's sub-processors are the following: