10 Lower Grosvenor Place
London, SW1W 0EN

+44 (0) 208 102 8000
optomany.com

DATA PROTECTION ADDENDUM

1. Each party acknowledges and agrees that for the purposes of the Data Protection Law and the Agreement:

1.1. Unless specified otherwise, the Customer shall be the Controller and the Supplier the Processor in respect of Personal Data for the purposes of Data Protection Law.

1.2. Notwithstanding anything to the contrary, in respect of the following circumstances, the Supplier shall act as Controller over the Personal Data:

1.2.1. where required for the purposes of Anti-Money Laundering and Fraud obligations;

1.2.2. to the extent required to comply with applicable legal obligations;

1.2.3. to the extent required to comply with the Card Scheme rules, or with any payment scheme rules or payment services agreement applicable to the Supplier.

1.3. When acting as a Controller, the Customer remains responsible for its compliance obligations under the Data Protection Law, and for the written Processing instructions it gives to The Supplier.

2. This **Error! Reference source not found.** applies to:

2.1. the Processing by a Party of Personal Data, in its capacity as a Processor, on behalf of the other Party (in its capacity as Controller) in the course of the performance of the Agreement with the Controller; and

2.2. the Processing by a Party of Personal Data, in its capacity as a Processor (including sub-Processor), on behalf of the Customer (in the Customer's capacity as Controller) in the course of the provision of the the Subscribed Services pursuant to the Agreement, and references in this **Error! Reference source not found.** to the 'Processor' shall be construed accordingly.

3. References in this **Error! Reference source not found.** to:

3.1. 'Personal Data' shall mean Personal Data which is Processed in each Party's capacity as pursuant to clause Each party acknowledges and agrees that for the purposes of the Data Protection Law and the Agreement:

3.2. Unless specified otherwise, the Customer shall be the Controller and the Supplier the Processor in respect of Personal Data for the purposes of Data Protection Law.

3.3. Notwithstanding anything to the contrary, in respect of the following circumstances, the Supplier shall act as Controller over the Personal Data:

3.3.1. where required for the purposes of Anti-Money Laundering and Fraud obligations;

3.3.2. to the extent required to comply with applicable legal obligations;

3.3.3. to the extent required to comply with the Card Scheme rules, or with any payment scheme rules or payment services agreement applicable to the Supplier.

3.4. When acting as a Controller, the Customer remains responsible for its compliance obligations under the Data Protection Law, and for the written Processing instructions it gives to The Supplier.

3.5. This **Error! Reference source not found.** applies to:;

3.6. 'Processing' has the meaning set out in the UK GDPR (and Process, Processes and Processed shall be construed accordingly).

4. Notwithstanding anything to the contrary in the Agreement, in the event of a conflict between any provisions of the Agreement and the provisions of this **Error! Reference source not found.**, the provisions of this **Error! Reference source not found.** shall take precedence. An overview of the categories of Personal Data, the categories of Data Subjects, and the nature and purposes for which the Personal Data are being Processed is provided in Annex 1 to this Schedule.

5. The obligations set out in this Data Protection Addendum shall survive termination of the Agreement.

6. Any capitalised terms or words defined in Data Protection Law and used in this Data Protection Addendum relating to Personal Data where such terms have not been defined in this Agreement shall, for the purposes of this Data Protection Addendum, have the meaning set out in Data Protection Law.

7. The Controller and the Processor

7.1. Subject to the provisions of the Agreement, to the extent that the Processor's Processing activities are not adequately described in the

Agreement, the Controller will determine the scope, purposes, and manner by which the Personal Data may be Processed by the Processor. The Processor will Process the Personal Data only as set forth in the Controller's written instructions and no Personal Data will be Processed unless explicitly instructed by the Controller.

7.2. The Processor will only Process the Personal Data on documented instructions of the Controller to the extent that this is required for the provision of the Subscribed Services. Should the Processor reasonably believe that a specific Processing activity beyond the scope of the Controller's instructions is required to comply with a legal obligation to which the Processor is subject, the Processor shall, to the extent permitted by applicable laws, inform the Controller of that legal obligation and seek explicit authorisation from the Controller before undertaking such Processing and shall be entitled to charge a reasonable fee for complying with such instructions. The Processor shall never Process the Personal Data in a manner inconsistent with the Controller's documented instructions. The Processor shall immediately notify the Controller if, in its opinion, any instruction infringes any applicable laws. Such notification will not constitute a general obligation on the part of the Processor to monitor or interpret the laws applicable to the Controller, and such notification will not constitute legal advice to the Controller.

7.3. The Parties have entered into the Agreement in order to benefit from the capabilities of the Processor in securing and Processing the Personal Data for the purposes set out in Annex 1. The Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, provided that all such discretion is compatible with the requirements of this **Error! Reference source not found.**, in particular the Controller's written instructions.

7.4. The Controller warrants that it has all necessary rights to provide the Personal Data to the Processor for the Processing to be performed in relation to the Subscribed Services, and that one or more lawful bases set forth in Data Protection Law support the lawfulness of the Processing. To the extent required by Data Protection Law, the Controller is responsible for ensuring that all necessary privacy notices are provided to Data Subjects, and unless another legal basis set forth in Data Protection Law supports the lawfulness of the

Processing, that any necessary Data Subject consents to the Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by a Data Subject, the Controller is responsible for communicating the fact of such revocation to the Processor, and the Processor remains responsible for implementing Controller's instruction with respect to the Processing of that Personal Data.

8. Confidentiality

8.1. Without prejudice to any existing contractual arrangements between the Parties, the Processor shall treat all Personal Data as confidential and it shall inform all its employees, agents and/ or approved sub-Processors engaged in Processing the Personal Data of the confidential nature of the Personal Data. The Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

9. Security

9.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security of the Processing of Personal Data appropriate to the risk. These measures shall include, at a minimum, the security measures agreed upon by the Parties in Annex 2.

9.2. Both the Controller and the Processor shall maintain written security policies that are fully implemented and applicable to the Processing of Personal Data. At a minimum, such policies should include assignment of internal responsibility for information security management, devoting adequate personnel resources to information security, carrying out verification checks on staff who will have access to the Personal Data, conducting appropriate background checks, requiring employees, vendors and others with access to Personal Data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the Personal Data aware of information security risks presented by the Processing.

10. Audit Rights

10.1. At the request of the Controller, the Processor shall demonstrate the measures it has taken pursuant to this Data Protection Addendum and shall allow the Controller to audit such measures no more than once a year, unless the Controller can demonstrate it suspects there has been a material breach by the Processor of its obligations under this Data Protection Addendum. Unless otherwise required by a Supervisory Authority of competent jurisdiction, the Controller shall be entitled on giving at least thirty (30) days' notice to the Processor to carry out, or have carried out, by a third party who has entered into a confidentiality agreement with the Processor, such audit under the present Clause 10.

10.2. Prior to conducting any audit pursuant to clause 10.1, the Controller must submit an audit request in writing to The Supplier and the Controller and The Supplier must agree the start date, scope and duration of and security and confidentiality controls applicable to any such audit.

10.3. The Supplier may (acting reasonably) object to the appointment by the Controller of an independent auditor to carry out an audit pursuant to clause 10.1 and, where this is the case, the Controller shall be required to appoint another auditor who is not (in the reasonable opinion of The Supplier) a competitor of The Supplier.

10.4. Any such audit will be limited to a document audit only and no in-person audits of The Supplier will be permitted to the fullest extent permitted by applicable law.

11. Improvements to Security

11.1. The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Processor will therefore evaluate the measures as implemented in accordance with clause 11 on an on-going basis in order to maintain compliance with the requirements set out in clause 11. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in Data Protection Law or by any Supervisory Authority.

11.2. Where an amendment to the Agreement is necessary in order to execute a Controller instruction to the Processor to improve security measures as may be required by changes in Data Protection Law from time to time, the Parties shall negotiate an amendment to the Agreement in good faith.

12. Data Transfers

12.1. The Processor shall promptly notify the Controller of any planned permanent or temporary transfers of Personal Data to a third country, including a country outside of the UK or European Economic Area (as applicable) without an adequate level of protection, and shall only perform such a transfer after obtaining authorisation from the Controller, which may be refused at its own discretion. Annex 1 provides a list of transfers for which the Controller grants its authorisation upon the conclusion of the Agreement.

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

13. Information Obligations and Incident Management

13.1. In the case of a Personal Data Breach, the affected Party shall without undue delay and, in any event, not later than twenty-four (24) hours after having become aware of it, notify the Personal Data Breach to the other providing the other with sufficient information which allows the Party to meet any obligations to report a Personal Data Breach under Data Protection Law

13.2. Where a Party becomes aware of any Personal Data Breach, it will, without undue delay, also provide the other Party with the following written information:

13.2.1. description of the nature of the Personal Data Breach including the categories of Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

13.2.2. the likely consequences; and

13.2.3. a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

13.3. Immediately following any accidental, unauthorised or unlawful Personal Data Processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Controller will reasonably co-operate with the Processor at no additional cost to the Processor, in the Processor's handling of the matter, including but not limited to:

13.3.1. assisting with any investigation;

13.3.2. making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Law or as otherwise reasonably required by the Processor; and

13.3.3. taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data Processing.

13.4. Any notifications made to the Controller pursuant to this clause 13 shall be addressed to the relevant employee of the Controller whose contact details are provided from time to time and, in order to assist the Controller in fulfilling its obligations under Data Protection Law, should contain:

13.4.1. a description of the nature of the incident, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

13.4.2. the name and contact details of the Processor's data protection officer or another contact point where more information can be obtained;

13.4.3. a description of the likely consequences of the incident; and

13.4.4. a description of the measures taken or proposed to be taken by the Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

14. Contracting with Sub-Processors

14.1. The Processor may subprocess any of its service-related activities consisting of (partly) of the Processing of the Personal Data or requiring Personal Data to be Processed by any third party, for which the Controller hereby gives its consent.

14.2. The Controller authorises the Processor to engage the sub-Processors for the Service-related Processing activities described in Annex 1.

14.3. Notwithstanding any authorisation by the Controller within the meaning of clause

14.4. The Controller authorises the Processor to engage the sub-Processors for the Service-related Processing activities described in Annex 1. , the Processor shall remain fully liable vis-à-vis the Controller for the performance of any such sub-Processor that fails to fulfil its data protection obligations.

14.5. The Processor shall ensure that the sub-Processor is bound by data protection obligations compatible with those of the Processor under this **Error! Reference source not found.**, shall supervise compliance thereof, and must in particular impose on its sub-Processors the obligation to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of Data Protection Law.

15. Returning or Destruction of Personal Data

15.1. Upon termination of the Agreement, upon the Controller's written request, or upon fulfilment of all purposes agreed in the context of the Services whereby no further Processing is required, the Processor shall, at the discretion of the Controller, either delete, destroy, make unavailable by permanently encrypting it, or return all Personal Data to the Controller or return any existing copies.

15.2. The Processor shall notify all third parties supporting its own Processing of the Personal Data of the termination of the Data Processing Agreement and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Controller, at the discretion of the Controller.

15.3. The Processor shall not be required to return or delete any Personal Data in accordance with clause 15.1 where it is required to retain such data in order to comply with applicable laws.

16. Assistance to Controller

16.1. The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights under the Data Protection Law.

16.2. Taking into account the nature of Processing and the information available to the Processor, the Processor shall reasonably assist the Controller in ensuring compliance with obligations pursuant to clause 16 and Annex 2, as well as other Controller obligations under Data Protection Law that are relevant to the Processing described in Annex 1, 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.

16.3. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the Processor's obligations and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

Error! Reference source not found.

Annex 1 - DATA PROCESSING INFORMATION

This Annex 1 to Data Protection Addendum includes certain details of the Processing of Personal Data as required by Article 28(3) GDPR.

Subject matter, nature and purposes of the Processing of Personal Data	The Supplier will process the Personal Data for the purposes of providing the SubscribedServices to the Customer in accordance with the Agreement. This may include sending transaction authorisation requests to Card Schemes and payment acquirers which act as Controllers (or Processors on behalf of Controllers) in their own right, and are not sub-Processors of the Supplier.
Duration of the Processing	The duration of the Agreement and such period following the Agreement until deletion or return of the Personal Data by The Supplier in accordance with the Agreement. Cardholder Data is retained for 5 years following a transaction to enable tokenisation, reporting and support enquiries
Type of Personal Data	Cardholder Data, as listed below (and associated Personal Data) of the Customer's customers as provided to The Supplier by (or at the direction of) the Customer (including by Card Schemes and relevant acquirers): • Primary account number; • email address of cardholder; • postal address of cardholder; • name of cardholder; • IP addresses of cardholder; • and geolocation data of cardholder.

Categories of Data Subjects	Customers, Cardholders
Sub-processors	The Supplier Affiliates, PaxStore, Microsoft Azure

Error! Reference source not found.

ANNEX 2 – SECURITY MEASURES

The Supplier shall implement the following technical and organisational measures to protect Personal Data against accidental loss and unauthorised access, disclosure or destruction:

1. Governance and policies

1.1. The Supplier assigns personnel with responsibility for the determination, review and implementation of security policies and measures.

1.2. The Supplier has documented the security measures it has implemented in a security policy and/or other relevant guidelines and documents.

2. Intrusion, anti-virus and anti-malware defences

2.1. The Supplier IT systems used to Process Personal Data have appropriate security software installed on them.

3. Access controls

3.1. The Supplier limits access to the Personal Data by implementing appropriate access controls. Access controls can include:

3.1.1. Requiring authentication and authorisation to gain access to IT systems (i.e. require users to enter a user ID and password before they are permitted access to the IT systems);

3.1.2. Only permit user access to Personal Data which the user needs to access in order to perform their job role or the purpose they are given access to The Supplier's IT systems;

3.1.3. Having in place appropriate procedures for controlling the allocation and revocation of access rights to the Personal Data. For example, having in place appropriate procedures for revoking employee access to IT system when they leave their job or change role.

4. Availability and back-up of Personal Data

4.1. The Supplier regularly backs up information on IT systems and keeps back-ups in separate locations.

5. Segmentation of Personal Data

5.1. The Supplier will, as appropriate, separate and limit access between network components and where appropriate implement measures to provide for separate Processing (storage, amendment, deletion, transmission) of Personal Data collected and used for different purposes.

6. Encryption

6.1. The Supplier uses encryption technology where appropriate to protect the Personal Data.

7. Transmission or transport of the Personal Data

7.1. Appropriate controls will be implemented by The Supplier to secure the Personal Data during transmission or transit.

8. Physical security

8.1. The Supplier implements physical security measures to safeguard Personal Data. Such measures may include:

8.1.1. buildings are appropriately secured;

8.1.2. measures taken to prevent Personal Data from being read, copied, amended or moved by any unauthorised persons;

8.1.3. hard copy documents containing Personal Data are only taken off site where necessary to achieve the purposes of the Agreement; and

8.1.4. paper records which contain confidential information (including Personal Data) must be shredded after use in accordance with industry standards.

9. Staff training and awareness

9.1. The Supplier carries out staff training on data security and privacy issues relevant to employees' job role and ensures that new starters receive appropriate training before they start their role (as part of the on boarding procedures).

9.2. Staff are subject to disciplinary measures for breaches of The Supplier's policies and procedures relating to data privacy and security.

10. Selection of service providers

10.1. The Supplier assesses service providers' ability to meet their security requirements before engaging them.

10.2. The Supplier has written contracts in place with service providers which require them to implement appropriate security measures to protect the Personal Data they have access to and limit the use of Personal Data in accordance with The Supplier's instructions.