Data Processing Agreement

Version 1.0, May 2022

This Data Processing Agreement (the "**DPA**"), presented below is the part of the Agreement between the Company (the "**Data Controller**") and Solidgate (the "**Data Processor**") that has the reference to this DPA and form an integral part of the Agreement.

1. DEFINITIONS

The following definitions shall apply in this DPA in addition to other defined in the Agreement; and, for the avoidance of doubt, in the event of any inconsistency or conflict, the applicable special definitions below shall supersede and/or amend the definitions in the Standard Clauses.

Data Controller	means the party that has authority over the processing of Personal Data, determining the purpose for its use and the manner that it is processed.
Data Processor	means the party that processes Personal Data on behalf of, and under the instruction of, the Data Controller.
Data Protection Authority	means the official body that ensures compliance with the Data Protection Laws within its applicable jurisdiction.
Data Subject	means the directly or indirectly identified or identifiable person to whom the Personal Data relates.
Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
Data Protection Laws	means all applicable laws, statues, regulations, ordinances, codes, rules, guidance, orders or any other legal entitlement issued by any governmental body governing the collection, use, transfer, and disclosure of Personal Data, including, if applicable, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
Employees	means employees, officers, consultants, suppliers, freelancers and individual subcontractors.
Personal Data	means any information regulated by Data Protection Laws, including information concerning an identified or identifiable individual, such as, name, address, age, gender, email address, etc., that is processed by the Data Processor on behalf of the Data Controller as a result of, or in connection with, the provision of the Services under the Agreement.
Processing, processes and process	mean either any activity that involves the use of Personal Data or as the Data Protection Laws may otherwise define processing, processes or process. It includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage,

	adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. Processing also includes transferring Personal Data to third parties.
Standard Contractual Clauses ("SCC")	means contractual clauses established by the European Commission concerning the international transfer of Personal Data, as set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 04 June 2021.
Sub-Processor	means the third party that may process personal data on behalf of Data Processor's obligations under the Agreement. Data Processor shall ensure that Sub-Processors comply with substantially same obligations as Data Processor under this Agreement. Data Processor remains responsible at all times for compliance with the terms of this Agreement.

2. GENERAL PROVISIONS

2.1. The Company attests that it is the Data Controller of Personal Data within the meaning of the Data Protection Laws and Solidgate determines that it will be acting as a Data Processor in respect of the Personal Data that is the subject of the Agreement.

2.2. Personal data processing shall be entrusted to the Data Processor for the purposes and period of the performance of the Agreement and/or until no further processing is required by the Agreement or Applicable Law.

2.3. The subject matter, duration, nature and purpose(s) of the processing of Personal Data, as well as type of Personal Data and categories of Data Subjects are specified in Annex A.

2.4. The Data Processor shall refrain from processing Personal Data that is beyond the scope set forth in Annex A.

2.5. In case the Data Processor receives additional information that is not needed to fulfil the Agreement, it must inform the Data Controller immediately and stop the processing of the additional Personal Data.

3. INSTRUCTIONS

3.1. The Data Processor shall process the Personal Data only on instructions from the Data Controller and for no other purpose than the purpose(s) defined in Annex A.

3.2. The Data Processor shall inform the Data Controller if, in its opinion, an instruction infringes the Data Protection Laws. The processing of the Personal Data required in said instruction shall be delayed.

3.3. If the Data Processor is required to transfer Personal Data to a law enforcement agency, it shall inform the Data Controller of that legal requirement before processing the Personal Data, unless that law prohibits such information on important grounds of public interest.

4. TECHNICAL AND ORGANISATIONAL MEASURES

4.1. The Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk before starting to process Personal Data.

4.2. In assessing the appropriate level of security, the Data Processor shall take into account the risks that are presented by Processing Person Data, in particular risks arising from a Data Breach.

4.3. The Data Processor undertakes to ensure the security of personal data entrusted for personal data processing in accordance with the Data Protection Laws and industry practices, in particular, to formulate and apply appropriate documentation and procedures for personal data processing, as well as technical, informational and legal security measures, as required by the Data Protection Laws, including inter alia:

4.3.1. the pseudonymisation and encryption of personal data;

4.3.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

4.3.3. the ability to restore the availability and access to personal data in a timely manner in the event of technical problems or any other incident;

4.3.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of personal data processing.

4.4. The Data Processor or its representative shall maintain a record (in writing or electronic form) of all categories of processing activities carried out on behalf of the Data Controller, containing:

4.4.1. the name and contact details of the Data Processor or its Sub-Processors and of the Data Controller, and, where applicable, of the Data Controller's or the Data Processor's representative, and the data protection officer;

4.4.2. the categories of Personal Data processing carried out on behalf of the Data Controller;

4.4.3. where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and including, where applicable, the documentation of suitable safeguards;

4.4.4. where possible, a general description of the technical and organisational security measures.

5. DATA PROCESSOR'S EMPLOYEES

5.1. The Data Processor shall ensure that all Employees with access to the Personal Data, are legally bound by confidentiality obligations during and after the termination of the DPA, including after the termination of their employment and/or other contractual arrangements with the Data Processor.

5.2. The Data Processor shall provide access to Personal Data to its Employees on a need-to-know basis only and shall make sure that the Employees are aware and compliant with the DPA, Data Controller's written instructions and the Data Protection Laws.

5.3. The Data Processor shall keep records of persons authorised for Personal Data processing.

5.4. The Data Processor shall train its Employees involved in the processing of the Personal Data to comply with the Data Protection Laws and with the requirements established in this DPA.

6. SUB-PROCESSORS

6.1. Data Controller authorizes Data Processor to appoint (and permit each Sub-Processor appointed in accordance with this clause 6 to appoint) Sub-Processors in accordance with this clause 6 and any restrictions in the Agreement.

6.2. The Data Controller hereby grants general written authorization to the Data Processor to engage an additional or replace existing Sub-Processors for the processing of the Personal Data under the Agreement. Upon request of the Data Controller, the Data Processor will provide a list of such Sub-Processors. The Data Controller has the right to object to any Sub-

Processor. The objection shall be made by written communication within 10 business days after receipt of requested list of Sub-Processors. The Data Processor shall use reasonable efforts to replace the Sub-Processor.

6.3. Where the Data Processor engages Sub-Processors, the Data Processor shall ensure that Sub-Processors comply with data protection obligations compatible with those of the Data Processor under this clause 6 as applicable to their processing of Personal Data. The Sub-Processor in particular shall provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Data Protection Laws. Where a Sub-Processor fails to fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the performance of that Sub-Processor's obligations.

7. DATA BREACHES

7.1. The Data Processor shall notify the Data Controller on Data Breach without undue delay. The notification shall include:

7.1.1. Description of the Data Breach, including, if possible, the categories of data and records concerned, the category and number of Data Subjects affected;

7.1.2. Likely consequences of the Data Breach;

7.1.3. Measures taken or proposed to address and/or mitigate the effects of the Data Breach.

7.2. The Data Processor shall, without undue delay, take all urgent measures as are agreed by the Parties or necessary under the Data Protection Laws, to investigate, mitigate and remedy the Data Breach and to protect the Personal Data.

7.3. Each Party needs the prior approval of the other Party to include and identify it in the breach notifications. The other Party should not delay or withhold the approval without a reasonable cause.

8. COOPERATION

8.1. Upon request, the Data Processor shall assist the Data Controller to comply with its obligations under the Data Protection Laws when related to the processing of the Personal Data, including but not limited to:

8.1.1. Data Breaches;

8.1.2. data protection impact assessments (DPIA);

8.1.3. consultations with the Data Protection Authority; and

8.1.4. enquiries, complaints, audits, or claims from any court, government official, or Data Protection Authority.

8.2. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in the Data Proctection Laws.

8.3. The Data Processor shall make available to the Data Controller all information necessary to comply with its obligations under the DPA and the Data Protection Laws.

8.4. The Data Processor shall notify the Data Controller of any requirements from an official authority as soon as possible.

8.5. The Data Processor shall assist the Data Controller in fulfilling its obligations concerning the requests to exercise Data Subject rights under the Data Protection Laws.

8.6. The Data Processor shall promptly transfer to the Data Controller any request received from the Data Subjects and shall inform the Data Subjects that they can direct their requests directly to the Data Controller. The Data Processor will only handle the requests of the Data Subjects according to the Data Controller's instructions.

9. AUDIT

9.1. Upon prior notice and no more than once a year, the Data Controller has the right to conduct an audit to verify the Data Processor's compliance with the DPA.

9.2. The Data Processor shall make available to the Data Controller documentation necessary to demonstrate compliance with this DPA and Data Protection Laws, in particular, to provide information about appropriate technical and organizational measures that have been implemented. The Parties agree that the Data Processor's attestation of compliance with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS) is sufficient for these purposes.

9.3. The Data Controller shall schedule the audit with the Data Processor at least 2 weeks in advance. The Parties shall agree upon the scope, the timing, and the duration of the audit.

9.4. The audit might be carried out by the Data Controller directly or by a third-party auditor appointed by the Data Controller. The Data Processor has the right to object the use of a particular third-party auditor, if it could be considered a competitor of the Data Processor.

10. CROSS-BORDER TRANSFER OF PERSONAL DATA

10.1. The Data Processor may transfer or otherwise process Personal Data outside the European Economic Area ("**EEA"**) without obtaining the Data Controller's prior written consent.

10.2. The Data Processor may only process, or permit the processing, of Personal Data outside the EEA under the following conditions:

10.2.1. the Data Processor is processing Personal Data in a territory in relation to which the European Commission has made an adequacy decision; or

10.2.2. the Parties have executed Standard Contractual Clauses.

10.3. If the transfer requires execution of the SCC, the unchanged version of the SCC shall be deemed incorporated by reference hereto and completed as follows:

10.3.1. Module Two will apply;

10.3.2. in Clause 7, the optional docking clause will apply;

10.3.3. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be at least 5 (five) business days;

10.3.4. in Clause 11, the optional language will not apply;

10.3.5. in Clause 17, Option 1 will apply, and the SCC will be governed by the law of Ireland;

10.3.6. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

10.3.7. Annex I of the SCC shall be deemed completed with the information set out in Annex A to this DPA and in the Agreement, Data Controller is the data exporter, Data Processor is the data importer;

10.3.8. Annex II of the SCC shall be deemed completed with the information set out in Annex B to this DPA and in the Agreement.

11. CALIFORNIA CONSUMERS PRIVACY RIGHTS

11.1. This Clause 11 is applicable to processing of Personal Information of Consumers. The terms "Personal Information" and "Consumer" shall have the meanings stipulated in the California Consumer Privacy Act of 2018, as amended from time to time ("**CCPA**").

11.2. The Data Processor shall not retain, use, or disclose Personal Information for any purpose other than for the specific purpose of performing the services specified in the Agreement.

11.3. The Data Processor shall not retain, use, or disclose Personal Information for a commercial purpose other than providing the services specified in the Agreement.

11.4. The Data Processor shall not retain, use, or disclose Personal Information outside of the direct business relationship between the Data Processor and the Data Controller

11.5. The Data Processor shall refrain from selling Personal Information, as the term "sell" is defined in the CCPA.

11.6. The Data Processor certifies that it understands the restrictions in Clauses 11.2 – 11.5 hereof and will comply with them.

12. TERMINATION

12.1. Termination of this DPA shall not affect Parties' accrued rights and obligations before or at the date of termination.

12.2. Upon the termination of the Agreement, whereby no further processing is required by the Agreement or Applicable Law, the Data Processor shall promptly return or irrevocably delete or remove the Personal Data.

12.3. The Data Processor may retain Personal Data to the extent required by Applicable Law and only to the extent and for such period as required by Data Protection Laws and always provided that Data Processor shall ensure the confidentiality of such Personal Data and shall ensure that such Personal Data is only processed as necessary for the purpose(s) specified in the Data Protection Laws requiring its storage and for no other purpose.

13. MISCELLANEOUS

13.1. In the case of conflict or ambiguity between:

13.1.1. any provision of the DPA and any other provision of the Agreement, the provisions of the DPA shall prevail;

13.1.2. any provision of this DPA and the SCC, the provisions of the SCC shall prevail.

solidgate

ANNEX A

DETAILS OF PERSONAL DATA PROCESSING

Subject matter of the processing of Personal Data:	The subject-matter of the data processing assignment is to enable End Users to perform payments on the Data Controller's website and/or other IT environments.
The nature the processing of Personal Data:	The scope of personal data processing shall include the following operations performed on the personal data: collecting, recording, storing, transferring, preparing, amending, making the data available, profiling with the use of personal data, deleting personal data both in paper form, as well as in the IT systems required for the provision of Services and for other purposes as may be required from time to time under the Agreement and Applicable Law.
The nature and purposes of the processing of Personal Data:	The Personal Data shall be processed to the extent necessary for provision of the Services by the Data Processor under the Agreement, namely, providing means for accepting payments made to the Data Controller using the Technical Solution and in compliance with Applicable Law, within the methods of payment handled by the Acquirer(s) and other services offered by the Data Processor to the Data Controller. Personal data of the Company's Representatives shall be entrusted to the Data Processor for the purpose of facilitating the process of Company's merchant processing account(s) opening and advising on its maintenance with applicable Acquirer.
The frequency and duration of the processing of Personal Data:	The Personal Data shall be processed on a continuous basis until no further processing is required by the Agreement or Applicable Law.
The categories of Data Subjects and Personal Data:	The types of personal data which will be processed by Data Processor under this Agreement may include: 1. Personal data of End Users: a. name; b. date of birth; c. phone number; d. IP address; e. email address; f. postal address; and g. data concerning transactions and payments, including, but not limited to, card transaction data. 2. Personal data of the Data Controller's Representatives: a. name; b. phone number; c. email address; d. residence address; e. id / passport details; f. tax number; g. bank details, personal income and source of wealth; h. employment history and education; i. ownership and directorship in the Company and/or other companies; j. adverse media and law enforcement information;

	k. presence in PEP, sanction, and watch lists; l. geolocation.
The obligations and rights of Data Controller:	The obligations and rights of Data Controller are set out in the Agreement and this DPA.
List of Parties:	The data exporter is the Data Controller and the address, contact details and activities relevant to the data transferred under the SCC are as provided in the Agreement. The data importer is the Data Processor and the address, contact details and activities relevant to the data transferred under the SCC are as provided in the Agreement.
Data Protection Authority:	If the Data Processor's contracting party is a legal entity incorporated in Cyprus – Office of the Commissioner for Personal Data Protection. If the Data Processor's contracting party is a legal entity incorporated in Gibraltar – Gibraltar Regulatory Authority.

solidgate

ANNEX B

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Certification or assurance of processes and products:	Data Processor maintains the PCI DSS certification throughout the term of this DPA.
Pseudonymisation and encryption of Personal Data:	Data Processor stores all Personal Data in encrypted form. Encryption and use are done by the HSM mechanism.
Ongoing confidentiality, integrity, availability and resilience of processing systems and services:	Data Processor ensures: - regular vulnerability scanning, - administrative access is allowed only through bastion sites, - access to systems is differentiated by the roles, - encryption keys are changed, and key and data access are reviewed on a regular basis. It is also possible to re-encrypt data in case of incidents.
The ability to restore the availability and access to data in the event of a physical or technical incident:	Data Processor maintains a recovery plan and ensures its periodic review and verification.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures:	Data Processor maintains a plan of periodic events: Daily, Weekly, Quarterly, Biannually, Annually, After Changes. All operations are audited annually.
User identification and authorisation:	Roles, personalized accounts and 2MFAs are used to access system management and administration. A policy on password complexity and frequency of password replacement is also applied. The duration of an inactive session is limited.
Personal Data protection during transmission:	Personal Data are transferred between systems using HTTPS TLS1.2 protocol.
Personal Data protection during storage:	Database storage and backups are encrypted with AES-256-GCM HSM keys.
Physical security of locations at which Personal Data are processed:	The Personal Data are stored on the AWS servers. The physical security of storage locations provided by AWS are compliant with standards: PCI DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171.
Events logging:	Operational events are recorded in persistence storage and monitored by monitoring systems 24/7. Infrastructure events are captured by AWS services such as: AWS CloudTrail and AWS GuardDuty.
Internal IT and IT security governance and management:	Internal security policies are maintained and regularly updated.
Limited data retention:	Storage systems and procedures are maintained to ensure timely deletion of Personal Data.