3 Legs Ltd, Lyonville, Stuggadhoo,
Marown, Isle of Man, IM4 2AJ

T 01624 626892
E sales@3Legs.com

Rev. June 2022
Company No: 100936C **VAT Reg Number:** GB001772610

Data Processing Agreement

This Data Processing Agreement (DPA) is an integral part of the Agreement (the "Agreement") or the Terms and Conditions for Service, between 3 LEGS LTD and Customer which includes the services listed below.

For the purposes of this DPA, the following definitions shall be understood as follows:

"GDPR" means General Data Protection Regulation.

"The Act" means the Isle of Man Data Protection Act 2018.

"Personal Data" means any information relating to an identified or identifiable natural person.

"Processing of Data" or "Processing" means any operation or set of operations performed on personal data, such as collection, recording, alteration, structuring, storage, adaptation, use, disclosure, making available or any other operation set out under the Isle of Man Data Protection Act 2018.

"Software" or "Database" shall mean any software or database provided directly or indirectly by 3 LEGS LTD or an Affiliate.

"SaaS" shall mean a web-based software service provided by 3 LEGS LTD in the form of a subscription fee.

"Customer" or "You" shall mean the User (as referred to in the Agreement) or the company, legal entity, or individuals providing professional services who purchase Licensed Services.

"Customer Data" means the information, (whenever or not including personal data), that the Controller uploads, transmits, inserts, or stores on the 3 LEGS LTD Software, hosted in a cloud environment.

"Services" or "Licensed Services" shall mean the hosting activity, email or SaaS, together with the technical support, maintenance and consulting services referred to.

For purposes of this DPA, You and 3 LEGS LTD agree that You are the controller and 3 LEGS LTD is the Processor of such Customer Data, and exceptionally when You act as a processor of Personal Data, 3 LEGS LTD will act as a sub-processor.

3 Legs Ltd, Lyonville, Stuggadhoo,
Marown, Isle of Man, IM4 2AJ

T 01624 626892
E sales@3Legs.com

Company No: 100936C **VAT Reg Number:** GB001772610

1. Subject matter and duration

1.1. Subject matter

The subject matter of this DPA results from the Licensed Services for any of the Software(s) or Database(s) that 3 LEGS LTD offers you in a dedicated or virtual environment.

Next to the hosting operation, 3 LEGS LTD may carry out support and maintenance/consulting activities in relation to the data collected and inserted by the Controller into the Database hosted in our systems:

- Maintenance and support of software products and possible 3rd-party products that are directly connected to services offered.
- Troubleshooting of software products and possible 3rd-party products directly connected to services offered.

1.2. Duration

The duration of this Data Processing Agreement corresponds to the duration of the Hosting Agreement to which it is attached.

2. Details of the Processing

2.1. Nature and Purpose of the Processing

Hosting:

The purpose of the activity is to offer Licensed Services for customers of the Software. The services provided to the Controller shall comprise:

- Set up of the system environment and application.
- Operation of the system environment and application.
- Installation of system patches.
- Installation of new application versions.
- Update of application Dictionaries.
- User Management.
- Backup of data and databases

Email

This activity is the provision of email mailboxes and SMTP services. The services provided to the Controller shall comprise:

- Set up of the system environment and application.
- Operation of the system environment and application.
- Installation of system patches.
- Installation of new application versions.
- Update of application Dictionaries.
- User Management.
- Storage of email in mailboxes that can be access via POP or IMAP.
- SMTP facilities for the sending of email from authorized email address.

- Backup of Mailbox

SaaS Services

This activity is the use by the client of one of our cloud-based software services provided as a subscription software service. The services provided to the Controller shall comprise:

- Set up of the system environment and application.
- Operation of the system environment and application.
- Installation of system patches.
- Installation of new application versions.
- Update of application Dictionaries.
- User Management.
- Storage of user information relevant to the given SaaS

1) Web Cart (also known as Security-Payment.net)

   a) User login details, basket contents, billing and delivery addresses

   - Data backup of the SaaS

Custom Software

This activity is the development and maintenance of a custom software solution. The services provided to the Controller shall comprise:

- Set up/Development of the software system environment and application.
- Maintenance of the software system environment and application.
- Installation of system patches.
- Installation of new application versions.
- Update of application Dictionaries.
- Data backup of the Software System

Support:

Additionally, 3 LEGS LTD may also perform technical support and assistance to 3 LEGS LTD's customers. In this case, the purpose is to provide technical assistance which encompasses support (at first, second and third level) with regards to the Software, usually via email, phone or web portal.

The customer's system can be accessed either remotely or directly at the customer's site. In particular, support activities may consist of the following:

- Error analysis and correction:

3 LEGS LTD can view various Log files for troubleshooting purposes. These are 3 LEGS LTD product-specific files, such as Trace/Log files, but also Log files generated by the system itself,
e.g., database Log files, or the event display of the operating system. Furthermore, visual access to files and information within the 3 LEGS LTD application and the corresponding database is possible.

- Maintenance and support:

During maintenance and support work, access to the web servers, the associated database and filing structures, as

well as to applications that are directly connected, can take place. Installation and uninstallation steps can be performed, as well as the modification and adaptation of configurations and configuration files which are required to operate the 3 LEGS LTD application.

Consulting:
During the performance of the Licensed Services, 3 LEGS LTD may also offer complementary services on request such as Consulting. Consulting services may include implementation, migration, validation and/or project management services. The Processing of the Customer Data will be executed in the same manner as when providing support services.

The customer's system can be accessed either remotely or directly at the Customer's site.

The undertaking of the contractually agreed Processing of Data will be carried out either in the Isle of Man or the UK.

2.2. Categories of Personal Data

The Processing activity comprises the following data types:

- Data related to the name, address, telephone and email address of the persons who place orders via any SaaS
- Data related to the collection of information from a website and stored in a database on the server
- Log and trace files of website hosting and email
- Data related sending and receiving of email

2.3. Categories of Data Subjects

The Data Subjects of the activity comprise the persons who use the websites, send emails, complete orders with SaaS or custom software systems for a given website or service, eventually further personal data from the Customer (see above).

3. Technical and Organisational Measures

3.1. Before the commencement of Processing, the Processor shall communicate the execution of the necessary Technical and Organisational Measures, specifically with regard to the execution of the contract, and shall present these measures to the Controller for inspection. Insofar as the inspection/audit by the Controller shows the need for amendments, such amendments shall be implemented by mutual agreement.

3.2. The Processor shall establish the security in accordance with The Act and GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of Processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons.

3.3. The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Processor to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

4.1. The Processor may not on its own authority rectify, erase or restrict the Processing of data that is being

processed on behalf of the Controller, but only on documented instructions from the Controller. Insofar as a Data Subject contacts the Processor directly concerning a rectification, erasure, or restriction of Processing, the Processor will immediately forward the Data Subject's request to the Controller.

4.2. Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Processor in accordance with documented instructions from the Controller without undue delay.

5. Quality assurance and other duties of the Processor

In addition to complying with the rules set out in this Order or Contract, the Processor shall comply with the statutory requirements; accordingly, the Processor ensures, in particular, compliance with the following requirements:

a) Appointed Data Protection Officer, who performs his/her duties in compliance with The Act & GDPR. His/Her current contact details are always available and easily accessible on the website of the Processor, and can be reached out through the following email address (privacy@3legs.com)

b) Confidentiality in accordance with The Act & GDPR. The Processor entrusts only such employees with the data Processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Processor and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Controller, which includes the powers granted in this contract, unless required to do so by law.

c) Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with The Act & GDPR.

d) The Controller and the Processor shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Controller shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the Processing of personal data in connection with the Processing of this DPA.

f) Insofar as the Controller is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data Processing by the Processor, the Processor shall make every effort to support the Controller.

g) The Processor shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that Processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the Technical and Organisational Measures conducted by the Controller as part of the Controller's supervisory powers referred to in item 7 of this contract.

6. Subcontracting

6.1. Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal/transport services, maintenance and user support services or the disposal of

data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data Processing equipment. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data, even in the case of outsourced ancillary services.

6.2. The Processor may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Controller.

a) The Controller agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with The Act & GDPR:

b)

Company Subcontractor	Service
Rackspace UK	Provider of Virtual Server Environment
Domicilium	Provider of Data Centre Services

Additional devices might be implemented in the Software:

Device (Company)	Function
PayPal	Processing of Online Payments
Trust Payment	Processing of Online Payments

c) Outsourcing to subcontractors or changing the existing subcontractor are permissible when:

- The Processor submits such an outsourcing to a subcontractor to the Controller in writing or in text form with appropriate advance notice; and
- The Controller has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Processor; and
- The subcontracting is based on a contractual agreement in accordance with GDPR.

6.3. The transfer of personal data from the Controller to the subcontractor and the subcontractor's commencement of the data Processing shall only be undertaken after compliance with all requirements has been achieved.

6.4. If the subcontractor provides the agreed service outside the EU/EEA, the Processor shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

6.5. Further outsourcing by the subcontractor requires the express consent of the main Controller (at the minimum in text form); All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Controller

7.1. The Controller has the right, after consultation with the Processor, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Processor in his business operations by means of random checks, which are

ordinarily to be announced in good time.

7.2. The Processor shall ensure that the Controller is able to verify compliance with the obligations of the Processor in accordance with GDPR**.** The Processor undertakes to give the Controller the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

7.3. Evidence of such measures, which concern not only the DPA, may be provided by either auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g., auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor), or a suitable certification by IT security or data protection auditing.

7.4. The Processor may claim remuneration for enabling Controller inspections.

8. Communication in the case of infringements by the Processor

8.1. The Processor shall assist the Controller in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in The Act & GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the Processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
b) The obligation to report a personal data breach immediately to the Controller
c) The duty to assist the Controller with regard to the Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Controller with all relevant information in this regard.
d) Supporting the Controller with its data protection impact assessment
e) Supporting the Controller with regard to prior consultation of the supervisory authority

8.2. The Processor may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Processor.

9. Authority of the Controller to issue instructions

9.1. The Controller shall immediately confirm oral instructions (at the minimum in text form).

9.2. The Processor shall inform the Controller immediately if he considers that an instruction violates Data Protection Regulations. The Processor shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

10. Deletion and return of personal data

10.1. Copies or duplicates of the data shall never be created without the knowledge of the Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data Processing, as well as data required to meet regulatory requirements to retain data.

10.2. After conclusion of the contracted work, or earlier upon request by the Controller, at the latest upon termination of the Service Agreement, the Processor shall hand over to the Controller or – subject to prior consent – destroy all documents, Processing and utilization results, and data sets related to the contract that have come into its possession, in a data protection-compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

3 Legs Ltd, Lyonville, Stuggadhoo,
Marown, Isle of Man, IM4 2AJ

T 01624 626892
E sales@3Legs.com
Company No: 100936C **VAT Reg Number:** GB001772610

10.3. Documentation which is used to demonstrate orderly data Processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Processor in accordance with the respective retention periods. It may hand such documentation over to the Controller at the end of the contract duration to relieve the Processor of this contractual obligation.

3 Legs Ltd, Lyonville, Stuggadhoo,
Marown, Isle of Man, IM4 2AJ

T 01624 626892
E sales@3Legs.com

Company No: 100936C **VAT Reg Number:** GB001772610

Attachment 1 - Technical and Organisational Measures

1. Confidentiality

- Physical Access Control
  No unauthorised access to Data Processing Facilities, e.g.: keys, electronic door openers, alarm systems
- Electronic Access Control
  No unauthorised use of the Data Processing and Data Storage Systems, e.g.: secure passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- Internal Access Control (permissions for user rights of access to and amendment of data)
  No unauthorised Reading, Copying, Changes or Deletions of Data within the system,
  e.g., rights authorisation concept, need-based rights of access, logging of system access events
- Isolation Control
  Isolated Processing of Data, which is collected for differing purposes through isolated productive, development and test systems; productive Data shall not be used as copy for test purposes; multiple Controller support, sandboxing.

2. Integrity

- Data Transfer Control
  No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN);
- Data Entry Control
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

3. Availability and Resilience

- Availability Control
  Prevention of accidental or willful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning
- Rapid;

4. Procedures for regular testing, assessment and evaluation

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default;
- Order or Contract Control
  No third-party data Processing as per GDPR without corresponding instructions from the Controller, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.