DATA PROTECTION ADDENDUM

1. RECITALS

1.1. This DPA sets forth the terms governing the Processing of Personal Data by the Licensor on behalf of the Licensee during the performance of Services under the Agreement.

1.2. The Parties agree that the:

1.2.1. Licensee is the Data Controller; and

1.2.2. Licensor is appointed as a Data Processor for Processing Personal Data solely to provide the Services, including transfers to jurisdictions outside the Licensee's country.

1.3. The terms of this DPA are binding and supplement the Agreement.

2. DEFINITIONS

In this DPA, unless the context clearly indicates a contrary intention, the following expressions shall bear the meaning assigned to them below, and cognate expressions shall bear corresponding meanings:

2.1. "**Agreement**" means the master service and license agreement entered into between the Parties, or to be entered into between the Parties contemporaneously with this DPA;

2.2. "**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to, or other unauthorised Processing of Personal Data transmitted, stored or otherwise processed;

2.3. "**Data Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

2.4. "**Data Processor**" means the natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller;

2.5. "**Data Protection Laws**" means any of the following laws on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data:

2.5.1. General Data Protection Regulations EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**");

2.5.2. the United Kingdom Data Protection Act, 2018;

2.5.3. the South African Protection of Personal Information Act, 2013 ("**POPIA**");

2.5.4. any data protection laws applicable to either of the Parties from time to time;

2.6. "**Data Subject**" means an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2.7. "**DPA**" means this data protection addendum;

2.8. "**Personal Data**" means any information relating to an identified or identifiable Data Subject;

2.9. "**Process/ing**" or "Processed" means 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;

2.10. "**Purpose**" means the provision of the Services and the associated Processing of Personal Data, as well as the Licensee's instruction provided to the Licensor during the use of the Services, the System or pursuant to the Agreement;

2.11. "**SCCs**" means the standard contractual clauses for the transfer of Personal Data to processors in third countries, approved by the European Commission from time to time, in the form set out in https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021D0914 to this DPA or as may be updated and approved by the European Commission from time to time; and

2.12. "**Sub-Processor**" means the entity engaged by the Licensor to Process Personal Data on its behalf and under its instructions from time to time, and for the time being as detailed in *Annexure B to the DPA*.

3. INTERPRETATION

Any term that is defined in the Agreement but not specifically defined in this DPA shall bear the meaning ascribed to it in the Agreement.

4. COMPLIANCE

During the term of this DPA, the Data Processor will comply with all applicable laws, regulations, regulatory requirements, and codes of practice when processing all Personal Data pursuant to its obligations under this DPA. These obligations specifically include complying with all the provisions of and any amendments to the applicable Data Protection Laws.

5. OBLIGATIONS OF LICENSEE

The Licensee agrees and warrants that, in relation to the Processing of Personal Data for the Purposes in the context of the Services, the Licensee acts as the Data Controller and therefore shall, to the extent permissible in terms of any Data Protection Laws:

5.1. provide lawful instructions for Processing Personal Data;

5.2. ensure Data Subjects are informed about Processing activities by the Licensor;

5.3. validate that there is a legal basis for Processing;

5.4. Avoid disclosing special categories of Personal Data unless explicitly agreed;

5.5. respond and comply to Data Subject rights requests and ensure data accuracy;

5.6. implement appropriate technical and organisational measures to secure Personal Data.

6. OBLIGATIONS OF DATA PROCESSOR

The Licensor agrees that, in relation to the Processing of Personal Data for the Purposes in the context of the Services, it acts as the Data Processor and therefore shall:

6.1. only Process, on the Licensee's behalf, Personal Data according to the Licensee's instruction and exclusively for the Purpose;

6.2. comply promptly with all such instructions that the Licensee communicates to the Licensor in writing, and the Licensor shall immediately inform the Licensee in writing if, in its opinion, an instruction infringes on any Data Protection Laws;

6.3. assist the Licensee in the fulfilment of the Licensee's obligation to respond to Data Subject requests (for example, the right to data portability, right of access, right to rectification, right of erasure, right to restrict Processing, right to object, and right to not be subjected to automated profiling);

6.4. promptly inform the Licensee, in writing if a Data Subject makes a data subject request directly to the Data Processor (for example, the right to data portability, right of access, right to rectification, right to erasure, right to restriction of Processing, right to object to Processing, and right to not be subjected to automated profiling), and the Data Processor must, as soon as it is reasonably possible to do so, notify the Licensee of this request and provide the Licensee with the details and information it requires to comply with its obligations under the applicable Data Protection Laws;

6.5. assist the Licensee in ensuring compliance with Data Protection Law obligations concerning data protection impact assessments;

6.6. assist the Licensee in ensuring compliance with Data Protection Law obligations and in responding to data protection authorities;

6.7. make available to the Licensee, all information necessary to demonstrate compliance with Data Protection Laws; and

6.8. subject to the Licensee's instructions, delete or return all Personal Data to the Licensee after the end of the Agreement and shall delete existing copies unless European Union or Member State law requires the storage of the Personal Data, where the Data Processor shall provide a written certification that it has complied herewith within ten days of termination of the Agreement.

7. SECURITY OF PROCESSING AND BREACH

7.1. The Licensor commits to maintaining a comprehensive information security program, incorporating technical and organisational measures that ensure a level of security appropriate to the risk. These measures include:

7.1.1. Encryption of Personal Data, ensuring ongoing confidentiality, integrity, and resilience of Processing systems and services, the ability to restore timely access to Personal Data following a physical or technical incident, and regular testing and evaluation of security measures to maintain their effectiveness.

7.1.2. Implementation of security measures assessed under applicable Data Protection Laws to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access, particularly during transmission over networks, ensuring security measures align with the state of the art, cost of implementation, and risks to Data Subjects' rights and freedoms.

7.1.3. Ensuring that individuals authorised to process Personal Data are bound by confidentiality agreements or appropriate statutory obligations.

7.2. In the event of a Data Breach, the Licensor will notify the Licensee without undue delay and, in any case, within 48 hours of becoming aware of the breach. The Licensor will take reasonable steps to mitigate the impact of the breach and minimise any resulting damage.

7.3. The Licensor will take all reasonable corrective actions and cooperate fully with the Licensee to address the breach. The Licensor will, subject to all applicable laws, provide the Licensee with the following reasonable details:

7.3.1. the nature of the breach, including, where possible, the categories and approximate number of Data Subjects and records affected;

7.3.2. the likely consequences of the breach; and

7.3.3. measures taken or proposed to mitigate the breach's effects and prevent its recurrence.

8. INTERNATIONAL DATA TRANSFERS

8.1. The Licensee acknowledges that the Licensor may transfer and Process Personal Data in the European Union, the United Kingdom or South Africa where the Licensor maintains data Processing operations.

8.2. The Licensor shall, at all times, ensure that such transfers are made in compliance with the requirements of the relevant Data Protection Law to a country that has been considered to provide an adequate level of protection under the Data Protection Law or to a data recipient which has implemented adequate safeguards under the Data Protection Law.

8.3. In particular, for transfers of Personal Data to the Licensor for Processing in a jurisdiction other than a jurisdiction in the European Union, the European Economic Area, or the European Commission-approved countries providing "adequate" data protection, the Licensor agrees to use the form of the SCCs.

9. SUB-PROCESSING

9.1. The Licensee gives the Licensor authorisation to engage the Sub-Processors for the Purpose. The Licensor shall inform the Licensee of any intended changes to the Sub-Processors in advance concerning the addition or replacement of other Data Processors, thereby giving the Licensee the opportunity to object to such changes. Where the Data Processor engages another Data Processor to carry out specific processing activities on behalf of the Licensee, the same data protection obligations as set out in this DPA shall apply.

9.2. To such Purpose, the Licensor represents that its Sub-Processors shall provide them sufficient guarantees to implement appropriate technical and organisational measures to ensure that their sub-processing will meet requirements under the applicable Data Protection Law, to the extent applicable to the nature of the services provided by such Sub-Processors.

9.3. The Licensor shall ensure that each Sub-Data Processor performs the obligations under this DPA as if it were party to this DPA in place of the Licensor.

10. AUDIT

10.1. Upon reasonable notice, the Licensee may audit the Licensor’s compliance with this DPA, including data security measures.

10.2. The Licensor will cooperate with such reasonable audits, provided they do not disrupt business operations or infringe on other clients’ confidentiality.

11. GENERAL

11.1. Save as set out in the DPA, the Agreement shall be and continue to be of full force and effect according to its tenor.

11.2. This addendum may be executed in any number of counterparts and by different Parties hereto in separate counterparts (in respect of which an electronic or facsimile copy thereof shall, *prima facie*, constitute a valid counterpart), each of which when so executed shall be deemed to be an original and all of which when taken together shall constitute one and the same addendum.

Description of Processing Activities

1. SUBJECT-MATTER OF PROCESSING

1.1. The Licensor is a web-based platform that gives companies the tools they need to manage lease accounting requirements.

1.2. The Licensor integrates lease accounting tasks and gives listed companies the capability to store and manage all lease contracts; account-for leases in line with the rules of IFRS 16; and report-on lease disclosures.

2. NATURE AND PURPOSE OF PROCESSING

The table below indicates the Purposes of the provision of Processing:

Yes/No	Purpose of business process	Explanation
Y	Lease Data Management	Processing of lease agreements and associated data to facilitate accurate compliance with accounting standards (e.g., IFRS 16).
Y	Client and User Account Management	Managing user accounts and client profiles for system access, support, and subscription purposes.
Y	Communication	Communication with clients regarding system updates, regulatory changes, and support inquiries.
Y	Reporting	Generating reports for accounting, compliance, and audit purposes as required by clients and stakeholders.

3. CATEGORIES OF DATA SUBJECTS

Employees, including consultants, temporary workers, independent contractors, and volunteers and directors and officers and other participants.

4. DURATION OF PROCESSING

The personal data may be stored for the period necessary to fulfil the intended Purpose for which the data was collected and further Processed unless otherwise required by applicable law.

5. TYPES OF PERSONAL DATA

The following types of personal data may be processed:

Types of Personal Data	Explanation	Yes / No
Subject Identification	Personal Identification Data	Yes
	Identification details issued by the government	No
	Electronic identification data	No
	Biometric identification data	No
Financial data	Financial identification data.	No
	Loans, credits	No
	Financial help	No
	Insurances	No
	Pension / retirement data	No
Personal characteristics	Personal details	Yes
	Military data	No
	Immigrant Status	No
Physical data	Physical description	No
Living habits	Substance use	No
	Lifestyle	No
	Travel	No
	Properties	No
	Public mandates	No
	Incidents or accidents	No
	Awards	No
Psychological data	Psychological description	No
Family status	Marriage or Cohabitation	No
	Details regarding other family members	No
Sound recordings		No

Types of Personal Data	Explanation	Yes / No
Memberships	Memberships (other than professional, political or trade union memberships)	No
Judicial information	Data on convictions and penalties	No
	information on judicial measures	No
Education and training	Curriculum	No
	Competences	No
	Professional experience	No
	Membership of / participation in professional organisations	No
	Publications	No
Employment	Current Employment	No
	Recruitment	No
	Termination of employment	No
	Presence and discipline	No
	Company medical service	No
	Salary, Wage	No
	Work organisation	No
	Evaluation	No
	Training	No
	Security	No
	IT tools	No
Racial or ethnic data		No
Political opinion	Political relationship	No
	Membership	No
Health data		No
Picture recordings	Pictures	No
	Surveillance camera	No

Annexure B to the DPA

Sub-Processors

Sub-Data Processor	Purpose	Location
Mailgun Technologies, Inc.	Email sending infrastructure	European Union
Amazon Web Services Inc.	Hosting & Infrastructure	European Union
Heroku	Platform-as-a-service	European Union
Microsoft Drive	Encrypted file storage	European Union

Technical and Organisational Measures

1. INTRODUCTION

1.1. The Licensor shall implement and maintain technical and organisational measures to protect against unauthorised or unlawful Processing of, or accidental loss, destruction, or damage to, the Personal Data, including all measures required by Article 32 of the GDPR and/or the relevant provisions of any Data Protection Law, as the case may be.

1.2. The Licensor shall implement the technical and organisational security measures set out herein.

2. SECURITY OVERVIEW

2.1. The Licensor uses Heroku, one of the world's leading Platform as a Service (“**PaaS**”) providers, to run the Licensor’s application. Heroku in turn uses Amazon Web Services (“**AWS**”), the world's largest cloud computing provider, for its infrastructure requirements.

2.2. The Licensor has selected that its servers are specifically based in the European Union Region (Ireland), where strict data protection policies are in place.

2.3. The Licensor's solution is fully hosted in Ireland, where it uses Amazon web services. The following services are used in this region: (i) web servers, (ii) database, (iii) background workers, and (iv) task queues. The Licensor’s database backups are located in the Frankfurt region of AWS.

2.4. AWS servers comply with the European Union protection directive. AWS servers have already obtained approval from the European Union data protection authorities, known as the Article 29 Working Party, of the AWS Data Processing Addendum and Model Clauses to enable the transfer of data outside Europe, including to the United States of America.

2.5. The AWS Data Processing Addendum is available to all AWS customers that are processing personal data whether they are established in Europe or a global company operating in the European Economic Area (available at https://aws.amazon.com/compliance/data-privacy-faq/).

3. USER SECURITY

3.1. Users of the System are required to select strong passwords which are encrypted before being stored in the database and uses industry-best-practice hashing algorithms.

3.2. In addition, all Users have the option to enable two-factor authentication for their own account. The Licensee can also select to enforce the two-factor authentication for all its Users.

4. LICENSOR SECURITY

4.1. All data in transit is encrypted using a secure sockets layer (SSL) or hypertext transfer protocol secure (HTTPS), including all data between the User's browser and the server, to protect sensitive data transmitted to and from the application.

4.2. Only two people at the Licensor have access to the servers.

4.3. Access to the servers is protected using double authentication mechanisms. To prevent unauthorised account access, the Licensor uses a strong passphrase for its Heroku user account and stores secure shell (SSH) keys securely to prevent disclosure.

4.4. The following protection mechanisms are in place by the Licensor:

4.4.1. cross-site scripting (XSS) protection;

4.4.2. cross-site request forgery (CSRF) protection;

4.4.3. security query language (SQL) injection protection;

4.4.4. click-jacking protection;

4.4.5. use of secure cookies;

4.4.6. secure password storage - passwords are never stored in plain text; and

4.4.7. platform as a service (PaaS) security standards.

4.5. Heroku applies security controls at every layer, from physical to application, isolating customer applications and data.

4.6. Heroku’s physical infrastructure is hosted and managed within AWS secure data centres, and it utilises AWS technology. AWS continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon’s data centre operations have been accredited under:

4.6.1. ISO 27001;

4.6.2. SOC 1 and SOC 2/SSAE 16/ISAE 3402 (previously SAS 70 Type II);

4.6.3. PCI Level 1;

4.6.4. FISMA Moderate; and

4.6.5. Sarbanes-Oxley (SOX).

4.7. Heroku utilises ISO 27001 and FISMA-certified data centres managed by AWS. AWS has many years of experience in designing, constructing, and operating large-scale data centres. This experience has been applied to the AWS platform and infrastructure. AWS data centres are housed in nondescript facilities, and critical facilities have extensive setbacks and military-grade perimeter control beams, as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilising video surveillance, state-of-the-art intrusion detection systems, and other electronic means. Authorised staff must pass two-factor authentication no fewer than three times to access data centre floors. All visitors and contractors are required to present identification, sign in, and continually be escorted by authorised staff.

5. FIREWALLS

5.1. Firewalls are utilised to restrict access to systems from external networks and between systems internally.

5.2. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

5.3. Host-based firewalls restrict customer applications from establishing local host connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

6. INFRASTRUCTURE

6.1. Heroku's infrastructure provides DDoS mitigation techniques, firewalls to prevent IP, MAC, and ARP spoofing on the network and between virtual hosts, and port scanning, which is prohibited.

6.2. Each application on Heroku runs within its own isolated environment and cannot interact with other applications or areas of the system.

7. DATA SECURITY

7.1. The Licensor has been subjected to security application and penetration tests and has also been tested against known vulnerabilities, using automated tool. The positive outcome of the penetration tests conducted on our system further reiterates our good security practices. Penetrations tests are completed from time to time by the Licensor.

7.2. The Licensor has strong access control policies in place to all services that it utilizes. Access to any part of its System is given to its staff only if it is a necessity. All access to either its System or third-party systems is protected through strong passwords and two factor authentication.

7.3. The Licensor has advanced error reporting and logging systems running in the background. Whenever any diagnostic test fails or a system bug is detected, emails are sent to the development team and these issues are prioritized. For all incidents, the Licensor follows a incident response policy.

7.4. Full-service level agreements are documented as part of the Agreement. This lays out all the particulars of support requirements from the Licensor, together with the client's obligations to receive different levels of support for different urgencies. The procedures and protocol is provided in the Agreement.

8. AMENDMENTS

The Licensor is permitted to implement other technical and organisational security measures equivalent to the measures prescribed in this *Annexure C to the DPA*.