1. PURPOSE OF THE CONTRACT

This agreement sets out the terms under which the Processor (E-Payroll (Mauritius) Ltd) provides a SaaS payroll solution on payrollmauritius.com (hereinafter the System) to the Controller (You) as the Data Protection Officer (or the Client: You), to assist the latter in processing personal data and other data relating to Data Subjects (see hereunder definition in 4.) in order to process their payroll independently, and how the Controller outsources to the Processor the hosting and automated processing of its Data Subject's data in accordance with the **Data Protection Act 2017**.

2. DURATION OF THE PROCESSING

Upon registering on the System, the Client's Controller and/or their legal representative have previously read and accepted this contract, thereby giving their explicit consent, which does not require a signature. Data processing continues for the entire duration of the SaaS contract and the 30 (thirty)-day cancellation period, unless the contract is terminated early in accordance with the stipulated terms. It remains in force for as long as the Controller/Client remains a customer of the System, by paying the monthly and/or annual subscription fees as defined in the System's pricing terms or in a specific contract signed between the Processor and the Controller, where applicable.

3. NATURE AND PURPOSE OF THE PROCESSING

Nature : The processing of Data Subjects' data involves the collection, recording, storage, retrieval, transmission (to tax authorities, social security bodies, data transmission subcontractors and banks) and deletion of the Client's Data Subjects' data.

Purpose : The purpose of the processing is to assist the Controller (not to replace nor act on their behalf) with payroll management, as well as the processing of working days and hours, leave, tax returns and social security contributions submitted to the Mauritius Revenue Authority (MRA or via MNS)), the National Pension Fund, the National Savings Fund, the Employee Welfare Fund, the generation of various management and HR reports, and the payment of salaries through the main Mauritian banks.

No personal data relating to employees is used for advertising, marketing or profiling purposes.

4. DATA SUBJECTS AND DATA

Data Subjects: The Data Subjects (hereinafter referred to as 'Data Subjects') concerned are the Client's current employees, former employees, trainees and (where applicable) job applicants who have been entered into the System

Data: The data processed (hereinafter referred to as the 'Data') relating to Data Subjects may include:

- **Personal informations**: surname, first name, nickname, marital status, passport photo, telephone number, address, date of birth, email address, password (if the Employee uses the Staff Connect mobile app or is a user of the System themselves), gender, NIC number, ID badge, landline and mobile phone numbers, bank

and bank account number, and, where applicable, the Data Subjects' dependants (first name, surname, gender and type of dependant) and, optionally (variable fields configurable by the Client), any information about the Data Subject that the Controller wishes to retain of their own accord and without the Processor being informed or held responsible (for example, and without limitation, passport, nationality, personal email, contact person, various preferences, etc.)

- **Job details**: Start date, end date, position held, type of employment contract, disciplinary warnings received, work schedules, Department and site of attachment, and any digital document (PDF, text, images, etc.) that the Controller wishes to retain in the System on an optional basis regarding the Data Subject of their own accord and without the Processor being informed or held responsible (for example, and without limitation, employment contract, bank details, electricity bills, etc.)

- **Working time information**: leave taken, days worked, dates and times of arrival at and departure from the workplace, geolocation coordinates of the clocking-in point (where supported by the clocking-in system)

- **Information relating to salary or used to calculate salary**: contributions to the NSF, CSG, PRGF or pension fund contributions, PAYE (income tax), PAYE exemption amount, date and time of submission of the EDF (Employee Declaration Form), basic salary, various bonuses and eligibility criteria, various deductions and how they are calculated, any deductions arising from loans, PDF files of payslips

5. THE CONTROLLER'S OBLIGATIONS

- Provide the Processor with documented instructions that are lawful and comply with applicable regulations;
- Ensure that there is a legal basis for the processing of individuals' data of Data Subjects;
- Inform the Data Subjects of the processing of their data;
- Ensure, in advance, that the processing complies with the Data Protection Act 2017.

In particular, the Data Controller is responsible for managing the departure of Data Subjects from the Company, deciding at their own discretion whether to retain, anonymise or delete the Data Subjects' data from the System.

The Controller is reminded of the Data Retention usage, under which Data's retention following a Data Subjects' departure must not exceed a 'reasonable' period in the event of a potential administrative request from the Mauritian regulatory authorities or a belated request from the Data Subject. A period of 5 + 1 years is generally accepted as such a reasonable period in the event of a Data Subject permanent departure.

6. OBLIGATIONS OF THE PROCESSOR

6.1 Processing on instruction

The Processor undertakes to process data solely on the basis of documented instructions from the Controller, unless otherwise required by law, and, by default, in accordance with the System settings configured by the Controller or authorised personnel of the Client.

The fact that the Controller, at its discretion, configures the System settings (or has them configured by authorised personnel of the Client) and/or uses those settings constitutes a specific instruction.

6.2 Privacy

The Data Controller ensures that staff authorised to process data undertake to maintain confidentiality or are subject to an appropriate legal obligation.

6.3 Data security

- The Processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

  - Hosting on servers hosted by Google© Cloud in the EU and compliant with ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, PCI DSS and CSA STAR standards, ensuring a high level of redundancy, resilience and compliance
  - Data encryption: SSL/TLS 1.2
  - 2048-bit HTTPS encryption and secure storage of SQL databases (256-bit AES encryption);
  - Access control; via Role-Based Access Control (RBAC), strong authentication and 2FA implementation
  - Logging; additions/modifications/deletions made to the system are logged (who, what, when) and can be viewed by the Controller
  - Secure API architecture
  - Disaster recovery plan (see SLA)
  - Secure backups performed within the EU (Belgium, Spain) and in Mauritius, redundant and encrypted.
  - Regular security tests; internal and external

6.4 Support for the Controller

The Processor assists the Controller, where possible, in:
- responding to requests from Data Subjects to exercise their rights (access, rectification, erasure, etc.);
- ensuring compliance with legal obligations (notification of breaches, impact assessments, etc.).

6.5 Notification of breaches

The Processor will notify the Controller as soon as possible (within 48 hours) after becoming aware of a personal data breach.

6.6 Data Subjects' rights

The Processor will assist the Controller in handling requests from Data Subjects regarding access, rectification, erasure, objections to processing and, more generally, any lawful requests made by Data Subjects or the relevant authorities.

7. SUBCONTRACTING

The Processor may not engage a subcontractor without the prior written authorisation of the Controller. At present, apart from the hosting provider Google® Cloud, the Mauritius Revenue Authority (MRA) and Mauritius Network Services (MNS) for tax payments, and the National Pension Fund, the National Savings Fund and the Employee Welfare Fund for social security contributions, and the banks for salary payments, no other sub-contractors have been authorised.

In the event of authorised subcontracting duly notified to the Controller, the Processor shall impose on such subcontractor the same obligations as those set out in this contract.

8. INTERNATIONAL TRANSFERS

International transfers are limited to:
- Hosting of resources, data and processing within the European Union (Belgium) via Google® Cloud
- Backing up of data in encrypted form (Spain)

9. END OF CONTRACT

Upon completion of the service, the Processor undertakes, at the Controller's discretion:
- either to return all personal data;
- and/or to delete (or anonymise) all personal data.

In all cases, the Processor shall delete all existing copies, unless there is a legal obligation to retain them.

10. AUDIT

The Controller reserves the right to carry out audits, or to have audits carried out, at its own expense, in order to verify the Processor's compliance with its obligations.

11. LIABILITY

Each Party is responsible for complying with its obligations under this contract and the Data Protection Act 2017.

12. APPLICABLE LAW

This contract is governed by Mauritian law.

If any provision of this contract is held to be invalid, the remaining provisions shall remain in full force and effect.

Any dispute arising out of or in connection with the interpretation or performance of this contract shall be submitted to the competent courts of the Republic of Mauritius.