DATA PROCESSING AGREEMENT

BETWEEN

COMPLIANCE SOFTWARE SOLUTIONS 2024 LIMITED (“COMPLY”) AND CUSTOMERS

Data Processing Agreement

This **Data Processing Agreement** ("Agreement") forms part of the Contract for Services ("Principal Agreement") between Customer and Compliance Software Solutions 2024 Limited (hereinafter referred to as "COMPLY") (the "**Data Processor/Processor**") ("together as the Parties").

WHEREAS

(A) The Customer acts as a Data Controller.

(B) The Customer wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with section 30 (5) of the Jamaica Data Protection Act, 2020 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Data Processing Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules and Annexes

1.1.2 "Customer" means the subscriber to the licensed use the Comply Software

1.1.3 "Customer Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Customer pursuant to or in connection with the Principal Agreement;

1.1.4 "Contracted Processor" means a Sub-processor;

1.1.5 "Data Protection Laws" means the Jamaican Data Protection Act, 2020, Data Protection (Data Controller Registration) Regulations 2024, The Data Protection Regulations and, to the extent applicable, the data protection or privacy laws of any other jurisdiction;

1.1.6 "DPA" means Data Protection Act, 2020;

1.1.7 “Data Transfer” means:

1.1.7.1 a transfer of Customer Personal Data from Processor to a Contracted Processor;

1.1.7.2 a transfer of Customer Personal Data from the Processor to a Third Country; or

1.1.7.3 an onward transfer of Customer Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.8 “Services” means any services provided by Processor including the Cloud Services, Support, Professional Services, and any other services set out in the Order Form.

1.1.9 “Sub-processor” means any person appointed by or on behalf of the Processor to process Personal Data on behalf of the Customer in connection with the Agreement.

1.2 The terms, “Information Commissioner”, “Controller”, “Data Subject, “Personal Data”, “Personal Data Breach”, “Processing” and shall have the same meaning as in the DPA, and their cognate terms shall be construed accordingly.

1.3 “Third Country” means a country outside of Jamaica which is not an Adequate Country.

2. Processing of Customer Personal Data

2.1 Processor shall:

2.1.1 Comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

2.1.2 Not Process Customer Personal Data other than on the relevant Customer’s documented instructions;

2.2 The Customer instructs Processor to process Customer Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual’s duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 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, Processor shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in section 30(6) of the DPA.

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

5. Sub-processing

5.1 Processor shall not appoint (or disclose any Customer Personal Data to) any Sub-processor unless required or authorized by the Customer.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1.1 promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

6.2.1.2 ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Customer without undue delay upon Processor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Customer and take reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with the Office of the Information Commissioner, which the Customer reasonably considers to be required by section 30(5)(b) of the DPA or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Audit rights

9.1 Subject to this section, a Processor shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Contracted Processors.

9.2 Information and audit rights of the Customer only arise under section 9.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

10. Data Transfer

The Processor may not transfer or authorize the transfer of Data to a Third Country without the prior written consent of the Customer. Prior to transfer, the Parties shall review the adequacy of data protection in the Third Country. The Parties shall apply any necessary appropriate measures to ensure that the personal data transferred will be subject to an equivalent level of protection as required under applicable data protection laws. To achieve this, the Parties shall, unless agreed otherwise, rely on approved standard contractual clauses and other security safeguards to ensure compliance for the transfer of personal data.

Deletion or Return of Data

Following termination of the Agreement, Customer shall have thirty (30) days to export all its Data from Cloud Services and after such Processor may delete its Data in its possession or control. This requirement shall not apply to the extent that (a) Processor is required by applicable law to retain some or all of the Data; or (b) Data is archived on Processor's back-up and support systems, which shall be deleted in accordance with its security procedures, provided that Processor shall continue to protect such Data in accordance with its obligations herein.

11. General Terms

11.1 **Confidentiality.** Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:
(a) disclosure is required by law; and
(b) the relevant information is already in the public domain.

11.2 **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

12. Governing Law and Jurisdiction

12.1 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of Jamaica.

12.2 Each party irrevocably agrees that the courts of Jamaica shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims), arising out of or in connection with this Agreement or its subject matter or formation.

This Agreement shall be effective as of the start date specified in the duly executed End User Order Form.

SCHEDULE A

Personal Data Processing Purposes and Details

Subject matter of processing	Names and Email Addresses
Duration of processing	For the Term of the Principal Agreement
Nature of processing	Data Discovery and Assessment Questionnaires
Business Purpose(s)	Services for Compliance with the Data Protection Act, 2020
Personal Data Categories	Identifying: (name; email address)
Authorised persons: an individual duly appointed by the Processor to act on its behalf in matters related to this Agreement and the Principal Agreement	
Identify the legal bases for processing the Personal Data ☒ For the performance of a contract with the data subject ☒ For compliance with a legal obligation ☐ To protect the vital interests of the data subject ☐ To exercise a function conferred by an enactment ☐ To exercise a function of a public nature in the public interest ☐ Legitimate interest ☐ Binding Corporate Rules ☐ Standard Contractual Clauses (stated which): ____ ☐ Other (describe in detail): ____	
Approved Subcontractors	
N/A	

SCHEDULE B

Security Measures

Supplier is to insert description of its technical and organizational data security measures, such as: Organisational Measures	Reporting Information Security Weaknesses, Response to and Learning from Information Security Incidents, Compliance with Legal and Contractual Requirements, Education and Training
System access controls	Logical Access Control, Encryption, Password Management System, Secure Log on Procedures, Fortinet Intrusion Detection System, Information Security Reviews, Information Security Risk Treatment
Data access controls	User Authentication, Authorization, Access Control Policy, User Access Management, User Registration and De-Registration, User Responsibilities
Transmission controls	Encryption in Transit, Regular Digital Certificate Management, Network Traffic and Log Monitoring
Input controls	Data Validation and Sanitization, Data Integrity and Consistency Checks, Encryption at Rest
Data backups	Daily Information Back-Up, Control of Operational Software
Data segregation	Logical segregation (multi-tenant architecture in our environment), Infrastructure-level segregation (cloud environment segregation)