DATA PROCESSING AGREEMENT

(AUDIT AND ASSURANCE SERVICES)

This Data Processing Agreement ("Agreement") is entered into on _____, 20_____ ("Effective Date").

BY AND BETWEEN:

Client: _____, with its principal place of business at _____ (hereinafter referred to as the "Data Controller"); and

Auditor: _____, with its principal place of business at _____ (hereinafter referred to as the "Data Processor").

The Data Controller and the Data Processor are collectively referred to as the "Parties" and individually as a "Party."

1. Background and Purpose

1.1. The Data Controller and the Data Processor have entered into an engagement letter or agreement dated _____ (the "Principal Agreement") under which the Data Processor agreed to provide audit, assurance, and related professional services (the "Services").

1.2. In the course of providing the Services, the Data Processor may process Personal Data on behalf of the Data Controller. This Agreement outlines the data protection, security, and privacy obligations of both Parties in accordance with applicable data protection laws.

2. Definitions

2.1. **"Applicable Data Protection Law"** means all legislation and regulations relating to the protection of personal data and privacy applicable to the processing of Personal Data under this Agreement.

2.2. **"Personal Data"** means any information relating to an identified or identifiable natural person processed by the Data Processor on behalf of the Data Controller in the performance of the Services.

2.3. **"Personal 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.

3. Scope and Subject Matter of Processing

3.1. The details of the processing operations, including the subject matter, duration, nature, and purpose of the processing, as well as the categories of Personal Data and Data Subjects, are specified in **Schedule 1** of this Agreement.

4. Obligations of the Data Processor

4.1. **Instructions:** The Data Processor shall process Personal Data only on documented instructions from the Data Controller, including with regard to transfers of Personal Data, unless required to do so by applicable law to which the Data Processor is subject.

4.2. **Confidentiality:** The Data Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.3. **Security Measures:** The Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk associated with processing Personal Data. These measures

shall, at a minimum, include the safeguards set forth in **Schedule 2**.

4.4. **Sub-processors:** The Data Processor shall not engage another processor (Sub-processor) without prior specific or general written authorization of the Data Controller. In the case of general written authorization, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other processors.

4.5. **Data Subject Rights:** Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organizational 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.

4.6. **Assistance:** The Data Processor shall assist the Data Controller in ensuring compliance with security obligations, breach notifications, data protection impact assessments, and prior consultations, taking into account the nature of processing and the information available to the Processor.

4.7. **Audit Rights:** The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

5. Personal Data Breach Notification

5.1. In the event of a Personal Data Breach, the Data Processor shall notify the Data Controller without undue delay, and in any event no later than _____ hours after becoming aware of the Personal Data Breach.

5.2. The notification shall contain, at minimum: a description of the nature of the breach, the categories and approximate number of data subjects concerned, the categories and approximate number of personal data records concerned, the likely consequences of the breach, and any measures taken or proposed to mitigate its effects.

6. Term and Termination

6.1. This Agreement shall remain in force for the duration of the Principal Agreement.

6.2. Upon termination of the Services, or at any time upon the Data Controller's request, the Data Processor shall, at the choice of the Data Controller, delete or return all Personal Data to the Data Controller and delete existing copies unless applicable law requires storage of the Personal Data.

7. Governing Law and Jurisdiction

7.1. This Agreement shall be governed by and construed in accordance with the laws of _____.

7.2. Any dispute arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts of _____.

For the Data Controller (Client):

_____

Name: _____
Title: _____
Date: _____

For the Data Processor (Auditor):

_____

Name: _____
Title: _____
Date: _____

Schedule 1: Details of Processing

Subject Matter of Processing	_____
Duration of Processing	_____
Nature and Purpose of Processing	_____
Categories of Personal Data	☐ Financial and accounting records ☐ Employee payroll and tax information ☐ Client/Customer contact details ☐ Identification and social security numbers ☐ Other (specify): _____
Categories of Data Subjects	☐ Employees / Staff members ☐ Customers / Clients ☐ Vendors / Suppliers ☐ Shareholders / Beneficial Owners ☐ Other (specify): _____

Schedule 2: Technical and Organizational Security Measures

The Data Processor shall implement and maintain the following security measures:

1. **Access Control:** Restricting access to Personal Data to authorized personnel who have a business need to access such data for the performance of the audit.
2. **Encryption:** Encrypting Personal Data both in transit and at rest using industry-standard cryptographic protocols.
3. **Transmission Security:** Utilizing secure, encrypted channels (such as secure client portals, SFTP) for any transmission of audit evidence and financial records.
4. **Data Integrity:** Implementing measures to protect Personal Data against unauthorized modification, deletion, or loss.
5. **Physical Security:** Restricting physical access to facilities, data centers, and paper files containing audit documentation.
6. **Security Assessments:** Regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented.