

## Standard Data Processing Addendum (DPA)

**Effective Date:** June 11, 2026

**Version:** 1.0 (Pre-Signed B2B Edition)

This Data Processing Addendum ("DPA") is entered into by and between the entity subscribing to the AccountScope services ("Controller" or "Firm") and AccountScope ("Processor", operated by VerdictOS Technology Ltd.). This DPA is incorporated into and forms part of the Terms of Service governing the use of the services. It is pre-signed by the Processor and is fully binding upon signup.

### 1. Definitions and Interpretation

---

- "Applicable Data Protection Laws" means all applicable laws and regulations relating to the processing of personal data, including the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018.
- "Personal Data", "Controller", "Processor", "Data Subject", "Processing", and "Supervisory Authority" shall have the meanings given to them under Applicable Data Protection Laws.
- "Subprocessor" means any third-party processor engaged by the Processor to assist in processing personal data on behalf of the Controller.

### 2. Scope and Role of the Parties

---

2.1. The parties acknowledge and agree that for the purposes of the Agreement, the subscribing customer is the Data Controller and AccountScope is the Data Processor. The details of the processing operations are:

- **Subject Matter:** The provision of bank statement transaction extraction, categorization, auditing, and financial remedy reporting services.
- **Duration:** The duration of the Agreement plus any post-termination retention periods defined in the Data Retention Policy.
- **Nature and Purpose:** To extract tabular transaction data from PDFs/CSVs, automatically group transactions into Form E categories, flag anomalies, and compile unified PDF reports.
- **Categories of Data Subjects:** Clients of the Controller, spouses/partners of those clients, dependent children, and individuals associated with transaction history details.
- **Types of Personal Data:** Names, physical addresses, bank account numbers, sort codes, transaction dates, descriptions, transaction amounts, and counterparty merchant names.

## 3. Obligations of the Processor

---

3.1. Instructions: Processor shall process personal data only on documented instructions from the Controller, including with respect to transfers of personal data to a third country or an international organization, unless required to do so by UK law.

3.2. Confidentiality: 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.

3.3. Security Measures: Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including PostgreSQL Row-Level Security (RLS), 256-bit encryption at rest, TLS 1.3 transit encryption, and configurable auto-purging schemes.

3.4. Subprocessors: Controller grants a general authorization to Processor to engage Subprocessors. Processor shall maintain an up-to-date list of Subprocessors at [accountscope.app/trust#subprocessors](https://accountscope.app/trust#subprocessors) and notify Controller of any changes 30 days in advance. Processor shall impose the same data protection obligations on any Subprocessor as set out in this DPA.

3.5. Data Subject Rights: Processor shall assist Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights.

3.6. Breach Notification: Processor shall notify Controller without undue delay, and in any event within 72 hours, after becoming aware of a personal data breach. The notification shall contain details of the breach, affected subjects, and mitigation steps.

3.7. Audit Rights: Processor shall make available to Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by the Controller.

3.8. Return or Deletion: At the choice of the Controller, Processor shall delete or return all personal data to the Controller after the end of the provision of services, and delete existing copies unless UK law requires storage of the personal data.

## 4. Obligations of the Controller

---

4.1. Controller warrants that it has all necessary consents, legal bases, and authority under Applicable Data Protection Laws to provide the personal data to the Processor and to instruct the Processor to process such data in accordance with the Agreement and this DPA.

4.2. Controller shall respond to Data Subject requests in accordance with Applicable Data Protection Laws.

## 5. Liability and Governing Law

---

5.1. The governing law of this DPA and any dispute arising out of it shall be the laws of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales.

## Execution and Sign-Off

---

### For the Controller (Firm):

Entity: Subscribing Organization

Name: [Authorized Signatory]

Title: Practitioner Representative

---

*Binding automatically upon account registration*

### For the Processor (AccountScope):

Entity: VerdictOS Technology Ltd.

Name: Compliance Desk Signatory

Title: Data Protection Officer

*/s/ Data Protection Officer*

---

*Pre-Signed & Electronically Validated*