ProcessLabs
Practical solutions for growing businesses

DATA PROCESSING AGREEMENT

Controller-to-processor terms

Version 5.0 | Effective 12 July 2026

PROCESS LABS AI SOLUTIONS LIMITED

Process Labs AI Solutions Limited (Company No. 17036074), registered in England and Wales. Registered office: 64 Nile Street, London, England, N1 7SR. ICO Registration: ZC094994.

Process Labs AI Solutions Limited (Company No. 17036074), registered in England and Wales. Registered office: 64 Nile Street, London, England, N1 7SR. ICO Registration: ZC094994.

This DPA applies only where ProcessLabs processes Personal Data on documented instructions as processor for the Customer. It does not apply to processing for which ProcessLabs is an independent controller.

1. Definitions and priority

Data Protection Legislation means the UK GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations 2003, Data (Use and Access) Act 2025 and applicable replacement or amending UK law. Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Processing and Special Category Data have their meanings in Data Protection Legislation.

If this DPA conflicts with the commercial Agreement on a data-protection matter, this DPA prevails. It does not expand commercial liability beyond the Agreement except where law requires.

2. Processing instructions

The Customer appoints the Company to process Personal Data only for the subject matter, duration, nature, purpose, types and Data Subjects in Schedule 1, the Order and documented instructions. The Company shall inform the Customer if an instruction appears unlawful, unless prohibited from doing so.

3. Customer obligations

The Customer warrants that it has a lawful basis, gives required notices, issues lawful instructions, minimises data, and has assessed whether the Services and security are appropriate. The Customer shall not provide Special Category or criminal-offence data without prior written agreement and documented safeguards.

4. Confidentiality and personnel

The Company shall ensure authorised personnel are bound by confidentiality, receive appropriate training and access Personal Data only as necessary.

5. Security

Taking account of state of the art, cost, scope, context, purpose and risk, the Company shall implement appropriate technical and organisational measures, including as appropriate access control, least privilege, encryption in transit, secure authentication, logging, backup or resilience controls, vulnerability management, incident response and secure deletion. Schedule 3 records the applicable measures and may be updated without materially reducing protection.

6. Subprocessors

The Customer gives general written authorisation for Schedule 2 subprocessors. The Company shall give at least 14 days' notice of an intended addition or replacement where reasonably practicable, allowing objection on reasonable data-protection grounds. If unresolved, the Company may use a reasonable alternative or either party may terminate the affected processing Service. The Company shall impose equivalent Article 28 obligations and remains responsible to the Customer for subprocessor compliance.

7. International transfers

The Company shall not make a restricted transfer unless permitted by Data Protection Legislation using adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to EU Standard Contractual Clauses, or another lawful safeguard, with any required transfer risk assessment and supplementary measures.

8. Data Subject requests

Taking account of the nature of processing, the Company shall provide reasonable technical and organisational assistance for the Customer to respond to Data Subject requests. If received directly, the Company shall forward it without responding except on Customer instruction or legal requirement.

9. Breach notification

The Company shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data and provide information reasonably available about nature, categories, likely consequences and mitigation. Notification is not an admission of fault. The Customer is responsible for regulator and Data Subject notifications unless law places the duty directly on the Company.

10. Assistance and compliance information

Taking account of processing and information available, the Company shall reasonably assist with security, breach assessment, DPIAs and prior consultation. It shall provide information reasonably necessary to demonstrate Article 28 compliance.

11. Audits

No more than once annually, and additionally after a material incident or regulator request, the Customer may audit relevant compliance on at least 20 Business Days' notice. The parties shall first use current independent reports and questionnaires where sufficient. On-site audit must be during business hours, avoid disruption and protect other customers. Customer bears cost unless material non-compliance is found. Auditor must be independent, competent and confidential.

12. Return and deletion

At the end of processing and at the Customer's choice, the Company shall return or delete Customer Personal Data and copies unless UK law requires retention. Data in protected backups may remain beyond active deletion where put beyond ordinary use and deleted on the next scheduled cycle. The default active-system deletion period is 30 days unless Schedule 1 states otherwise.

13. AI and training restriction

The Company shall not use Customer Personal Data to train, fine-tune or improve a general-purpose AI or machine-learning model. It may process data through an approved AI subprocessor solely to provide the Services under binding terms and documented instructions. Testing and evaluation using Customer Personal Data requires an instruction in Schedule 1 and must not train a general-purpose model.

14. Direct legal duties

Nothing in this DPA relieves either party of direct statutory obligations or liabilities. Each party is responsible for regulatory complaints relating to its own controller processing, including the complaints procedure required by applicable law.

Schedule 1: Processing details

Field	Details
Subject matter	As stated in the Order/SOW, or complete here: _____
Duration	As stated in the Order/SOW, or complete here: _____
Nature and purpose	As stated in the Order/SOW, or complete here: _____
Data types	As stated in the Order/SOW, or complete here: _____
Data Subject categories	As stated in the Order/SOW, or complete here: _____
Documented instructions	As stated in the Order/SOW, or complete here: _____
Retention and deletion	As stated in the Order/SOW, or complete here: _____
Special Category / criminal data safeguards	As stated in the Order/SOW, or complete here: _____

Schedule 2: Approved subprocessors

Provider	Service	Location / transfer safeguard	Data involved
To be completed and maintained on the current subprocessor list			

The Company must not name or imply a provider until its actual appointment, location, terms and transfer position have been verified.

Schedule 3: Technical and organisational measures

- Role-based and least-privilege access
- Multi-factor authentication where supported
- Encryption in transit and appropriate encryption at rest
- Secure credential handling and prohibition on credentials in ordinary AI prompts
- Supplier due diligence and contractual controls
- Logging, monitoring and incident response
- Data minimisation and retention controls
- Business continuity and tested restoration appropriate to the Service
- Staff confidentiality and awareness
- Vulnerability and patch management for systems within Company control

Execution

For Process Labs AI Solutions Limited	For the Customer
Signature: _____ Name: _____ Title: Director / Authorised Signatory Date: _____	Signature: _____ Name: _____ Title: Authorised Signatory Date: _____