DATA PROCESSING AGREEMENT (DPA)

Intelligent Automation Hub (Pty) Ltd
Reg. No. 2022/744946/07
Trading as: Intelligent Automation Hub (iAhub)
Physical Address: 26 Melville Road, Illovo, Sandton, 2196, South Africa
Domains: iahub.ai, iahub.co, intelligentautomationhub.co.za, intelligentautomationhub.com

1. Purpose of this Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of any agreement or engagement between:

- **The "Responsible Party"** (the customer or partner), and
- **Intelligent Automation Hub (Pty) Ltd** ("iAhub", "Operator", "Processor", "we", "us")

and governs the processing of personal information in terms of the **Protection of Personal Information Act (POPIA)** and any applicable international data protection laws.

The purpose of this DPA is to ensure that all processing activities performed by iAhub on behalf of the Responsible Party are lawful, secure, confidential, and aligned with POPIA's requirements.

2. Definitions

For purposes of this DPA:

- **"POPIA"** means the Protection of Personal Information Act 4 of 2013.
- **"Personal Information"** means any information relating to an identifiable natural or juristic person as defined under POPIA.
- **"Processing"** means any operation involving personal information, including collection, storage, use, transmission, or disposal.
- **"Responsible Party"** means the party that determines the purpose and means of processing.
- **"Operator / Processor"** means iAhub, which processes information on behalf of the Responsible Party.
- **"Sub-processor"** means any third party engaged by iAhub to assist with processing activities.
- **"Data Subject"** means any natural or juristic person whose information is processed.

3. Roles and Responsibilities

3.1 iAhub's Responsibilities (as Operator / Processor)

iAhub shall:

- Process personal information **only** as instructed by the Responsible Party.
- Maintain the confidentiality of all personal information.
- Implement appropriate **technical and organisational security measures**.
- Ensure that staff with access to data are subject to confidentiality obligations.
- Notify the Responsible Party of any data breach without undue delay.
- Cooperate with investigations or assessments conducted by the Responsible Party.
- Delete or return personal information upon termination of the agreement.
- Maintain records of processing activities as required by POPIA.

3.2 Responsible Party's Responsibilities

The Responsible Party confirms that:

- All instructions given to iAhub will comply with applicable laws.
- It has lawful justification for collecting and sharing personal information.
- It will ensure that its customers, staff, and end-users are informed of processing activities.
- It is responsible for decisions regarding data classification and retention periods.

4. Nature and Purpose of Processing

iAhub processes personal information for the following purposes, depending on the services provided:

- Implementation, configuration, support, and management of digital systems
- AI agents, automation, CX/EX solutions, and workflow orchestration
- Managed services, SaaS support, hosting, data migration, analytics, integration
- Monitoring, logging, diagnostics, and system optimisation
- Business operations, invoicing, reporting, and project delivery

Personal information processed may include, but is not limited to:

- Names, email addresses, phone numbers
- User profiles and authentication details
- System usage data and logs
- Customer tickets, conversations, or communication history
- Employee or operational records (where provided)
- Data from third-party platforms such as Freshworks, Zoho, Exotel, n8n, ElevenLabs, etc.

5. Categories of Data Subjects

Depending on the services provided, data subjects may include:

- Customer employees
- Client end-users
- Consumers, shoppers, or retail customers
- Website visitors, subscribers, and digital users
- Employees of the Responsible Party
- Contractors, suppliers, and partners
- Job applicants and candidates

6. Security Measures

iAhub will implement and maintain security measures including:

- Encryption of data in transit and at rest
- Multi-factor authentication and access controls
- Secure hosting infrastructure and private cloud environments
- Role-based access and least-privilege principles
- Regular patching, updates, and vulnerability assessments
- Secure backups and disaster recovery policies
- Audit logs, monitoring, and incident response systems
- POPIA and InfoSec training for all personnel

Detailed technical policies may be made available to the Responsible Party upon request.

7. Use of Sub-Processors

iAhub may engage third-party sub-processors for specific services, including:

- Cloud providers
- Software vendors and SaaS platforms
- AI engines and automation frameworks
- Telephony, messaging, and communications services
- Data storage or hosting providers
- IT support contractors

iAhub commits to:

- Only using sub-processors bound by POPIA-aligned agreements
- Ensuring appropriate security standards
- Remaining liable for acts or omissions of sub-processors

A list of key sub-processors can be supplied on request.

8. International and Cross-Border Transfers

Personal information may be transferred to or hosted in regions outside South Africa where services require it.

iAhub ensures:

- Transfers occur under POPIA's Section 72 requirements
- Sub-processors outside South Africa provide adequate safeguards
- Data remains protected to a standard similar to POPIA
- Cross-border risks are communicated and managed

Where required, the Responsible Party may request a list of such locations.

9. Confidentiality

iAhub shall keep all personal information strictly confidential and may not:

- Disclose it to any unauthorised third party
- Use it for any purpose other than delivering contracted services

Confidentiality obligations continue after the termination of the agreement.

10. Data Subject Requests

If iAhub receives a request from a Data Subject relating to:

- Access
- Correction
- Deletion
- Objection
- Data portability

iAhub will immediately forward the request to the Responsible Party unless authorised to respond directly.

11. Data Breach Notification

In the event of a suspected or confirmed data breach:

- iAhub will notify the Responsible Party **without undue delay**, including:
    - Nature of the breach
    - Categories and volume of data affected
    - Likely consequences
    - Mitigation measures taken or proposed
- iAhub will cooperate with investigations, containment efforts, and reporting obligations.

The Responsible Party is responsible for notification to Data Subjects and the Information Regulator unless otherwise agreed.

12. Audits and Compliance Reviews

The Responsible Party may:

- Conduct reasonable audits or assessments
- Request documentation demonstrating compliance
- Review security, privacy, and processing controls

Audit scheduling must consider operational impact and may incur a reasonable fee where applicable.

13. Data Retention and Deletion

Upon termination:

- iAhub will delete, anonymise, or return all personal information
- Secure deletion methods will be used
- Backup systems may retain encrypted copies for disaster recovery for a limited duration
- Records required by law may be retained as needed

14. Liability

iAhub shall not be liable for:

- Processing performed in accordance with the Responsible Party's instructions
- Inaccurate data provided by the Responsible Party
- Breaches caused by third-party systems not under iAhub's control

- Failures of infrastructure, platforms, or service providers outside iAhub's environment

The Responsible Party indemnifies iAhub for any losses arising from unlawful instructions or failure to comply with POPIA obligations.

15. Term and Termination

This DPA:

- Takes effect when incorporated into an agreement, quote, proposal, or SOW
- Remains effective for the duration of the engagement
- Survives termination to the extent required for confidentiality and data protection obligations

16. Governing Law

This DPA is governed by the laws of the **Republic of South Africa**.
Any disputes are to be resolved under South African jurisdiction.

17. Contact Details

Information Officer:
Name: Charles Lalieu
Email: charles@aihub.ai
Phone: +27 83 643 3377
Address: 26 Melville Road, Illovo, Sandton, 2196