CROSS-BORDER DATA TRANSFER ADDENDUM (CBTA)

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

1. Purpose of This Addendum

This Cross-Border Data Transfer Addendum ("Addendum", "CBTA") applies when **Intelligent Automation Hub (Pty) Ltd** ("iAhub") processes, transfers, hosts, or makes personal information accessible outside the Republic of South Africa on behalf of the "Responsible Party" (the customer or partner).

This Addendum forms part of:

- Any Master Services Agreement (MSA)
- Any Data Processing Agreement (DPA)
- Any Statement of Work (SOW)
- Any proposal, quotation, or project engagement

It ensures compliance with Section 72 of the **Protection of Personal Information Act, 4 of 2013 (POPIA)** regarding cross-border transfers.

2. Definitions

In this Addendum:

- **"Personal Information"** has the meaning defined in POPIA.
- **"Responsible Party"** is the party for whom iAhub processes data.
- **"Operator / Processor"** is iAhub.
- **"Cross-Border Transfer"** means any movement or access to personal information outside South Africa.
- **"Sub-processor"** means any third-party engaged by iAhub to process personal information.

3. Legal Basis for Cross-Border Transfers

iAhub may transfer or make personal information accessible outside South Africa only under one or more of the following POPIA-compliant bases:

1. The receiving jurisdiction has **adequate data protection laws**.
2. The **data subject consents** to the transfer.
3. The transfer is **necessary** for:

    - Contract performance
    - Provision of services
    - Implementation of technology or integration requirements
4. The foreign recipient is subject to a **binding agreement** that provides:
    - A level of protection equivalent to POPIA
    - Security and confidentiality
    - Lawful and restricted processing
5. The transfer is necessary for the **benefit of the data subject**, and it is not reasonably practical to obtain consent.

iAhub ensures compliance with one or more of these conditions before facilitating any cross-border transfer.

4. Types of Cross-Border Transfers Covered

Transfers may include, but are not limited to:

- Hosting of systems or data on international cloud platforms
- AI/LLM engines operating in global regions
- Voice and communication platforms (e.g., Exotel, Twilio)
- SaaS solutions (e.g., Freshworks, Zoho, ElevenLabs)
- Workflow automation platforms (e.g., n8n Cloud)
- Backup and disaster recovery sites
- Support access by international engineers
- Analytics, logging, and monitoring systems

Transfers may occur through:

- Remote system access
- API integrations
- Data synchronisation
- Storage or caching
- Technical support or troubleshooting

5. Responsibilities of iAhub (Operator / Processor)

iAhub shall:

- Ensure all cross-border transfers comply with POPIA Section 72.

- Verify that third-party platforms implement **adequate safeguards**.
- Enter into **POPIA-aligned agreements** with all sub-processors outside South Africa.
- Inform the Responsible Party of any material changes in the transfer environment.
- Implement security controls for all cross-border processing.
- Limit access to authorised personnel only.
- Ensure international support personnel are bound by confidentiality and security obligations.
- Maintain records of all cross-border processing activities.

6. Responsibilities of the Responsible Party

The Responsible Party acknowledges that:

- Many cloud and SaaS solutions used in digital transformation inherently rely on cross-border infrastructure.
- The Responsible Party is responsible for ensuring lawful collection of data before it is transferred.
- Instructions involving the use of foreign-hosted platforms constitute authorisation for cross-border transfers.
- If the Responsible Party restricts cross-border transfers, some services or functionalities may not be available.

The Responsible Party indemnifies iAhub for unlawful processing resulting from incorrect or incomplete instructions.

7. Locations of Cross-Border Processing

Depending on the platforms used, personal information may be stored or processed in (but not limited to):

- European Union (Ireland, Germany, Netherlands, France)
- United Kingdom
- United States of America
- India
- Singapore
- Australia
- United Arab Emirates
- Other AWS, Azure, or GCP global regions

A detailed list of sub-processors and hosting regions is available on request.

8. Sub-Processors and Third-Party Platforms

iAhub may engage sub-processors outside South Africa to provide services, including:

- Freshworks (CX/EX/SaaS platforms)
- Zoho Corporation
- Exotel and voice integration platforms
- ElevenLabs (voice AI)
- OpenAI and other LLM vendors (depending on configuration)
- AWS, Azure, Google Cloud
- n8n cloud and automation platforms
- Payment processors
- Logging, monitoring, and security services

All sub-processors must:

- Provide equivalent levels of protection to POPIA
- Sign binding agreements with iAhub
- Process data strictly according to iAhub's instructions

iAhub remains **fully liable** for any sub-processor it appoints.

9. Security Measures

iAhub shall ensure:

- Encryption in transit and at rest
- Network and API security controls
- Secure authentication and access management
- Role-based and least-privilege access
- Secure developer and operations practices
- Monitoring, logging, and incident response
- Disaster recovery and redundancy architecture
- Regular audits and vulnerability testing

Security documentation may be shared with the Responsible Party upon request.

10. Data Subject Rights in Cross-Border Environments

iAhub will support the Responsible Party in responding to requests relating to:

- Access
- Correction
- Deletion
- Objection
- Restriction
- Portability

Where the request involves foreign-hosted systems, iAhub will coordinate with international partners to facilitate compliance.

11. Breach Notification

If any security breach affects personal information transferred outside South Africa, iAhub shall:

- Notify the Responsible Party **without undue delay**
- Provide details of:
    - The nature of the breach
    - Systems or regions affected
    - Data subjects impacted
    - Remediation steps
    - Recommended mitigation measures

iAhub will fully cooperate with incident management and reporting obligations.

12. Return, Retention, and Deletion of Data

Upon termination or request:

- iAhub will delete or return all personal information stored cross-border.
- Data may remain temporarily in encrypted backups due to platform constraints.
- Retention will comply with legal, regulatory, and contractual obligations.

13. Liability

iAhub is not liable for:

- Processing required to perform services based on the Responsible Party's instructions

- Failures of third-party platforms where iAhub is not the developer or host
- Restrictions imposed by foreign data protection laws
- Losses arising from prohibited transfers initiated by the Responsible Party

The Responsible Party indemnifies iAhub against:

- Claims related to unlawful instructions
- Incomplete or incorrect data
- Lack of lawful basis for transfer

14. Governing Law

This Addendum is governed by the laws of the **Republic of South Africa**.
Disputes fall under South African jurisdiction.

15. Contact Information

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