EXTERNAL DATA PRIVACY AND SECURITY POLICY

Of
INTELLIGENT AUTOMATION HUB (Pty) Ltd AND ITS AFFILIATES
(Collectively referred to as **"Intelligent Automation Hub Group"** or **"the Group"**)

In accordance with:
The Protection of Personal Information Act 4 of 2013 (POPIA)
and, where applicable,
The General Data Protection Regulation (EU) 2016/679 (GDPR)

1. COPYRIGHT NOTICE

2. DEFINITIONS

2.1 "Group", "Company", "we", "us" or "our" refers to Intelligent Automation Hub (Pty) Ltd and **any subsidiary, affiliate, division, operating brand, joint venture partner, or entity under common ownership or control**, whether currently existing or formed/acquired in the future.

2.2 "Data Subject" means any identifiable natural or juristic person whose Personal Information is processed by the Group.

2.3 "Personal Information" means any information relating to an identifiable person or entity, including but not limited to:

- Name, identity/passport numbers, contact details
- Banking, financial, and transactional information
- Employment, academic and professional data
- Biometric identifiers, CCTV images
- IP addresses, cookies, browsing patterns

2.4 "Special Personal Information" includes race, ethnic origin, health, biometric data, sexual life, religious beliefs, or criminal behaviour.

2.5 "Processing" means any operation performed on Personal Information, including: collection, use, retention, storage, transmission, analysis, distribution, archiving, anonymisation, and destruction.

2.6 "Responsible Party" means the Group entity that determines the purpose and means of Processing.

2.7 “Operator / Processor” means a third party who processes information for or on behalf of the Group.

2.8 “Information Officer” refers to the appointed role under POPIA (may include Deputy Information Officers).

3. APPLICATION OF THIS POLICY

This Policy applies to:

- Clients and prospective clients
- Suppliers and service providers
- Employees of clients and partners
- Website and platform users
- Contractors, subcontractors, and external agents
- Any third party whose information we receive or process

This Policy applies **group-wide**, across **all jurisdictions**, including digital, cloud and cross-border systems used to deliver services.

4. PURPOSES FOR PROCESSING PERSONAL INFORMATION

The Group processes Personal Information only for **lawful, legitimate and specific purposes**, including:

4.1 To verify identity, perform due diligence, vendor onboarding and client authentication.
4.2 To enter into, manage and perform contractual obligations.
4.3 To deliver consulting, technology, managed services, support, platforms, solutions and related services.
4.4 To administer invoices, billing, transactions, accounting and tax compliance.
4.5 To manage service delivery, support tickets, SLAs and operational workflows.
4.6 To comply with legal, regulatory, audit and record-keeping requirements.
4.7 For cybersecurity monitoring, threat intelligence, access control and fraud prevention.
4.8 To secure physical premises, assets, networks and confidential information.
4.9 For employee, subcontractor and vendor management.
4.10 For marketing, stakeholder communication and relationship management where consent applies.
4.11 For research, performance analytics, service enhancement and innovation.
4.12 To support internal corporate governance, acquisitions, restructuring, mergers and due diligence.

5. INFORMATION WE COLLECT

We may collect:

Category	Examples
Identity & Contact Data	Full name, email, mobile, company details, ID/passport
Contract & Commercial Data	Purchase orders, proposals, agreements, billing info
Technical Data	IP address, device identifiers, browser data, log files, usage data, cookies
Security Data	CCTV footage, building access logs, authentication logs
Financial Data	Bank account details, payment history, tax information
Employment / Professional Data	CVs, qualifications, verification results
Communications	Emails, call notes, system messages, chatbot interactions

6. HOW PERSONAL INFORMATION IS COLLECTED

We collect Personal Information:

- Directly from Data Subjects
- Through automated digital interactions
- From client organisations
- From contracted third-party Operators (verification, analytics, hosting, security)
- From open/public records

7. SHARING OF INFORMATION

Personal Information **may be shared** with:

- Group employees and authorised stakeholders
- Third-party service providers and cloud hosting partners
- Business partners involved in delivery of customer solutions
- Regulators, auditors, legal authorities when required by law
- Law enforcement in the event of criminal investigation
- Potential merger/acquisition stakeholders under confidentiality controls

All Operators are bound to **confidentiality, data security and POPIA/GDPR** compliance.

8. CROSS-BORDER DATA TRANSFERS

Due to the nature of cloud and SaaS platforms used by IA Hub, Personal Information may be transferred or stored outside South Africa.

Where this occurs, the Group applies:

- **GDPR Standard Contractual Clauses (SCCs)**
- POPIA Section 72 Transfer Safeguards
- Encryption, access controls and contractual data protection obligations

No transfer will occur to jurisdictions lacking adequate safeguards unless legally permitted security controls are in place.

9. INFORMATION SECURITY

The Group applies **multi-layered** security controls including:

- Access control and RBAC authentication
- Encryption in transit and at rest
- Segmented network and zero-trust architecture
- Incident response and breach notification procedures
- Regular penetration testing and system patching
- Employee training on privacy and confidentiality

No system can be guaranteed entirely secure, but IA Hub continuously improves governance, controls and monitoring.

10. RETENTION AND DESTRUCTION

We retain Personal Information:

- Only for as long as legally or contractually required, or
- As necessary to fulfil the purpose for which it was collected

Once no longer needed, data is:

- **Securely destroyed**, or
- **Anonymised** where continued analytics value exists

11. DATA SUBJECT RIGHTS

Data Subjects may exercise the following rights:

- Request **access** to Personal Information
- Request **correction** or **updating**
- Request **deletion** (subject to legal retention limits)
- Withdraw consent where consent is relied upon

- Object to processing on legitimate grounds
- Request **data portability**
- Lodge a complaint with the Information Regulator

Requests must be submitted in writing to:
privacy@iahub.co.za

12. CHANGES TO THIS POLICY

This Policy may be updated periodically. The latest version is available on request or via formal communication channels.

13. CONTACT DETAILS

Intelligent Automation Hub (Pty) Ltd
26 Melville Road, Sandton, 2196, Gauteng, South Africa
privacy@iahub.co.za

Information Regulator (South Africa):
https://www.justice.gov.za/inforeg