



DRA GROUP PRIVACY NOTICE

DRA (Pty) Ltd
2021/916057/07

DRA-00-CL-POL-0002

Revision: 3

APPROVAL

Description	Name	Title	Signature	Date
Approved	James Smith	Chief Executive Officer		15 September 2026

REVISION RECORD

Revision	Description	Date
0	First issue	28 August 2019
1	General review	15 October 2021
2	General review and renamed from Privacy Policy to Website Privacy Policy	20 March 2023
3	Website Privacy Policy renamed to Privacy Notice. Privacy Notice updated to reflect company name change from DRA Global Limited to DRA (Pty) Ltd and to align with the Group's governance processes, strategy and operating model	15 September 2026

TABLE OF CONTENTS

1	INTRODUCTION	4
2	WHO THIS PRIVACY NOTICE APPLIES TO	4
3	WHO IS RESPONSIBLE FOR YOUR PERSONAL DATA	5
4	PERSONAL DATA WE COLLECT	5
5	HOW WE COLLECT PERSONAL DATA	5
6	LAWFUL BASIS FOR PROCESSING PERSONAL DATA	6
7	WHY WE PROCESS PERSONAL DATA	6
8	SHARING YOUR PERSONAL DATA	6
9	INTERNATIONAL / CROSS-BORDER TRANSFERS OF PERSONAL DATA	7
10	ARTIFICIAL INTELLIGENCE	7
11	INFORMATION SECURITY	7
12	RETENTION OF PERSONAL DATA	8
13	YOUR DATA PRIVACY RIGHTS	8
14	KEEPING YOUR PERSONAL DATA ACCURATE	9
15	CHILDREN'S PERSONAL DATA	9
16	THIRD-PARTY WEBSITES	9
17	DATA SECURITY INCIDENTS	9
18	CONTACT US	9
19	CHANGES TO THIS PRIVACY NOTICE	9

1 INTRODUCTION

DRA (Pty) Ltd and its controlled entities, subsidiaries, affiliates, branches and representative offices (collectively referred to as "the DRA Group", "DRA", "we", "our" or "us") are committed to protecting the privacy, confidentiality and security of personal data entrusted to us.

This Privacy Notice explains how we collect, use, disclose, store and otherwise process personal data when data subjects interact with the DRA Group.

This Notice applies to personal data collected through:

- Attendance at meetings, conferences and events;
- Client, supplier and contractor relationships;
- Communications with DRA;
- Employment relationships;
- Our business operations and services;
- Our websites and digital platforms;
- Recruitment and employment processes;
- Visits to our offices and project sites; and
- Any other interaction with the DRA Group.

The DRA Group operates internationally and processes personal data in many countries. We are committed to complying with the applicable data protection and privacy laws wherever we operate.

Where local data protection and privacy laws provide additional protections or rights, those requirements will apply in addition to this Privacy Notice.

2 WHO THIS PRIVACY NOTICE APPLIES TO

This Privacy Notice applies to any data subject (as defined by applicable data protection and privacy laws) whose personal data the DRA Group processes, including (but not limited to):

- Business partners;
- Contractors and consultants;
- Employees;
- Job applicants;
- Joint venture representatives;
- Members of the public who contact DRA;
- Prospective and existing clients;
- Representatives of customers and suppliers;
- Regulators;
- Shareholders and investors;
- Suppliers and service providers;
- Visitors to DRA premises; and
- Visitors to our websites.

3 WHO IS RESPONSIBLE FOR YOUR PERSONAL DATA

Depending on your relationship with the DRA Group and the country in which your personal data is processed, different DRA Group entities may act as the:

- Data Controller/Responsible Party;
- Business/Organisation; or
- Equivalent legal role,

under applicable data protection and privacy laws.

The relevant DRA Group entity responsible for your personal data will generally be the entity with whom you interact.

4 PERSONAL DATA WE COLLECT

The personal data we collect depends upon your interaction with the DRA Group.

Examples may include:

- **Business Information** – company details, professional role, correspondence, contractual information.
- **Contact Information** – postal address, residential address, telephone number, email address.
- **Employment Information** – CVs, qualifications, licences, certifications, employment history, referee information.
- **Financial Information** – bank account details, taxation information, payment information.
- **Identity Information** – name, title, date of birth, identification numbers, passport details, nationality.
- **Security Information** – CCTV footage, visitor records, access control records, security incident information.
- **Sensitive Personal Data / Special Category Data** – where authorised by applicable data protection and privacy laws or with the appropriate legal basis, DRA may process sensitive personal data / special category data, including information relating to: health, disability, criminal background checks, biometric identification, racial or ethnic origin, trade union membership, and/or other information protected by applicable data protection and privacy laws.
- **Technical Information** – IP address, browser information, device identifiers, operating system, website usage information.

5 HOW WE COLLECT PERSONAL DATA

We may collect personal data:

- Directly from you;
- From your employer or organisation;
- From publicly available sources;
- From service providers;
- From business partners;
- From regulatory authorities;
- Through our websites;
- Through our contractual relationships;
- Through recruitment agencies; and
- Through security and access control processes.

6 LAWFUL BASIS FOR PROCESSING PERSONAL DATA

Where required by applicable data protection and privacy laws, the DRA Group processes personal data on one or more lawful grounds, including:

- Compliance with legal obligations;
- Consent;
- Legitimate business interests;
- Performance of a contract;
- Protection of vital interests;
- Public interest; and
- Any other lawful basis recognised by applicable law.

7 WHY WE PROCESS PERSONAL DATA

We process personal data only for legitimate business purposes, including (but not limited to):

- **Business operations** – delivering engineering, project management, construction management, operations management and related services, consulting and advisory services, project execution, contract management, procurement and supplier management.
- **Client relationships** – responding to enquiries, providing services, managing customer relationships and client communications.
- **Communications** – newsletters, marketing communications (where permitted), investor communications, event management.
- **Employment administration** – workforce management, payroll, benefits, training, compliance.
- **Health, safety and security** – site access, workplace safety, incident investigations, emergency management, CCTV.
- **Legal and regulatory compliance** – compliance with applicable laws, engaging with regulators, legal proceedings, cyber-related requirements, due diligence and other (as required).
- **Recruitment** – recruitment, candidate assessment, onboarding.
- **Website administration** – website security, analytics, improving user experience and troubleshooting.

8 SHARING YOUR PERSONAL DATA

We may share personal data with:

- Auditors;
- Banks;
- Cloud service providers;
- Courts;
- DRA Group companies worldwide;
- Government authorities;
- HR and recruitment providers;
- Insurers;
- IT service providers;
- Joint venture partners;

- Law enforcement agencies;
- Legal services providers;
- Payroll providers;
- Professional advisers;
- Regulatory authorities; and
- Any other third parties acting on our behalf.

Where third parties process personal data on our behalf, they are required to maintain appropriate security measures and comply with applicable data protection and privacy laws.

9 INTERNATIONAL / CROSS-BORDER TRANSFERS OF PERSONAL DATA

As an international organisation, the DRA Group may transfer personal data between countries in which we operate.

Where personal data is transferred internationally/cross-border, we implement appropriate safeguards in accordance with applicable data protection and privacy laws, which may include (but are not limited to):

- Adequacy decisions;
- Approved transfer mechanisms;
- Contractual safeguards;
- Organisational measures; and
- Technical security controls.

10 ARTIFICIAL INTELLIGENCE

The DRA Group may use artificial intelligence technologies to improve business efficiency, assist with information management and support operational activities.

Where artificial intelligence technologies are used to process personal data, DRA will do so responsibly and in accordance with applicable data protection and privacy laws and its AI Governance Framework.

The DRA Group does not make solely automated decisions that produce legal or similarly significant effects on data subjects. Should this change, DRA will implement appropriate safeguards required by applicable law.

11 INFORMATION SECURITY

The DRA Group maintains appropriate technical and organisational security measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Our security measures include (but are not limited to), where appropriate:

- Access controls;
- Employee training;
- Encryption;
- Incident response procedures;
- Multi-factor authentication;
- Monitoring;
- Network security;
- Regular security testing;

- Third-party security assessments; and
- Vulnerability management.

12 RETENTION OF PERSONAL DATA

We retain personal data only for as long as necessary to:

- Comply with legal obligations;
- Fulfil the purposes described in this Notice;
- Protect legal rights;
- Resolve disputes; and
- Satisfy business requirements.

When personal data is no longer required, it will be securely deleted, destroyed or anonymized.

13 YOUR DATA PRIVACY RIGHTS

Depending upon your country of residence and applicable data protection and privacy laws, you may have rights to:

- Access your personal data;
- Be informed;
- Data portability;
- Lodge a complaint with the relevant supervisory or data protection authority;
- Object to processing;
- Object to direct marketing;
- Request correction;
- Request deletion;
- Request human review of automated decisions;
- Restrict processing; and
- Withdraw consent.

Not all rights apply in every country.

To exercise any of your rights or to make an enquiry regarding the processing of your personal data, please contact us using the contact details provided in Section 19 of this Privacy Notice.

To protect your privacy and the security of your personal data, we may ask you to verify your identity before processing your request. Where necessary, we may request additional information to enable us to locate the relevant records or confirm your authority to act on behalf of another data subject.

We will acknowledge and respond to your request within the timeframes required by applicable data protection and privacy laws. Where permitted by applicable data protection and privacy laws, we may charge a reasonable fee for providing access to your personal data or for processing requests that are manifestly unfounded, excessive or repetitive. Any applicable fee will be communicated to you before your request is processed.

If we are unable to fulfil your request, in whole or in part, we will explain the reasons for our decision and, where applicable, advise you of any rights you may have to seek a review, lodge a complaint with the relevant supervisory or data protection authority, or pursue any other remedy available under applicable law.

14 KEEPING YOUR PERSONAL DATA ACCURATE

We encourage data subjects to notify us promptly if their personal data changes so that our records remain accurate and complete.

15 CHILDREN'S PERSONAL DATA

The DRA Group does not knowingly collect personal data from children except where permitted or required by applicable law and with the necessary authorisations.

16 THIRD-PARTY WEBSITES

Our websites may contain links to third-party websites.

DRA is not responsible for the privacy practices or content of external websites and encourages users to review the privacy notices of those websites.

17 DATA SECURITY INCIDENTS

The DRA Group maintains procedures for identifying, managing and responding to personal data security incidents.

Where required by applicable data protection and privacy laws, the DRA Group will notify the relevant supervisory or data protection authority and affected data subjects of a personal data security incident.

The central reporting channel for suspected or actual data security incidents is:

Business Unit	Email
All Business Units	databreach@draglobal.com

18 CONTACT US

Questions regarding this Privacy Notice or requests relating to personal data should be directed to the relevant Data Protection Officer.

Business Unit	Email
APAC	APACDPO@draglobal.com
EMEA and SENET	EMEADPO@draglobal.com
Ghana	DRAGhanaDPO@draglobal.com
Minopex	MinopexDPO@minopex.com
NAMER	NAMER.privacy@draglobal.com
SAMER	SAMER.privacy@draglobal.com
Saudi Arabia	DRASaudiDPO@draglobal.com
Tanzania	ThamaniDPO@draglobal.com
Zimbabwe	DRAZimDPO@draglobal.com

19 CHANGES TO THIS PRIVACY NOTICE

We may update this Privacy Notice from time to time to reflect changes in our business operations, technologies, legal requirements or privacy practices.

The latest version will always be available on our website (www.draglobal.com) and will indicate the date on which it became effective.