Plera®

Privacy Policy & Data Protection

Legal

Privacy Policy & Data Protection Agreement

Effective Date: 1st May 2025
Last Updated: 1st May 2025

This Privacy Policy and Data Protection Agreement ("Agreement") outlines how Plera (Pty) Ltd ("Company," "we," "our," or "us") collects, uses, stores, and protects personal information in compliance with the Protection of Personal Information Act (POPIA) and applicable international data protection laws, including GDPR where applicable.

1. DEFINITIONS

1.1 "Personal Information" – Any information relating to an identifiable individual, including but not limited to name, contact details, business information, and IP addresses.
1.2 "Data Subject" – The individual or entity whose data is collected.
1.3 "Processing" – Any operation performed on Personal Information, including collection, storage, retrieval, use, and deletion.
1.4 "Third Party" – Any external service provider, vendor, or subcontractor handling data on behalf of the Company.
1.5 "Public Data" - Information that is publicly available through legitimate sources such as company websites, professional social networks, business directories, and other publicly accessible platforms.
1.6 "Aggregated Data" - A collection of public data consolidated into our proprietary database for business purposes.

2. INFORMATION OFFICER

2.1 As required by POPIA, we have designated an Information Officer who is responsible for ensuring compliance with applicable data protection laws.
2.2 Our Information Officer can be contacted at: **zwen@plera.co**

3. INFORMATION WE COLLECT

We may collect the following types of Personal Information:
3.1 From clients, prospects, and website users:

- Contact Information (name, email, phone number, business address)
- Business Details (company name, industry, LinkedIn profile data)
- Payment Information (billing details, invoicing data, payment methods)
- Usage Data (IP address, device information, browsing activity on our website)
- Communications (email correspondence, messages, support requests)

3.2 For our database and cold outreach services:

- Publicly available business contact information
- Professional profiles and work history from public sources
- Company information and business relationships
- Industry-specific data points relevant to our clients' needs

4. HOW WE COLLECT INFORMATION

We collect Personal Information through:

- Direct interactions (e.g., when clients sign up for our services, contact support, or make a purchase)
- Automated technologies (e.g., cookies, tracking technologies on our website)
- Third-party sources (e.g., business directories, professional networks)
- Public sources (e.g., company websites, professional social media profiles, business registries)
- Data enrichment services (with appropriate legal basis)
- AI-assisted data collection tools that process publicly available information

5. LEGAL BASIS FOR PROCESSING

We process Personal Information under the following legal bases:

- Contractual Necessity – To fulfill our obligations in providing services.
- Legitimate Interest – To improve our services, conduct analytics, communicate with clients, and perform business-to-business marketing activities.
- Legal Compliance – To meet regulatory obligations.
- Consent – When required, we obtain explicit consent before processing certain data.

6. HOW WE USE PERSONAL INFORMATION

We use Personal Information for the following purposes:

- To deliver and manage our lead generation and appointment-setting services.
- To develop and maintain our proprietary database of business contacts.
- To conduct cold outreach and facilitate sales activities on behalf of our clients.
- Communicate with clients regarding contracts, billing, and service updates.
- To improve our platform, analytics, and AI-driven workflow solutions.
- To train and optimize our AI messaging systems (using anonymized data where appropriate).
- To comply with legal and regulatory requirements.
- To prevent fraud, abuse, or security breaches.
- To onboard and manage sales agents and their activities.

7. DATA SECURITY & RETENTION

7.1 Security Measures

We implement industry-standard security measures to protect Personal Information from unauthorized access or breaches. All employees and agents undergo regular data protection training.

7.1.1 Cloud Storage

We utilize Google Workspace (including Google Sheets) and other enterprise-grade cloud service providers to store and process our aggregated data. These providers:

- Maintain ISO 27001 certifications and other security compliance standards
- Implement advanced encryption for data in transit and at rest
- Offer comprehensive physical, network, and system security
- Provide regular security updates and vulnerability management

We implement strict access controls, including:

- Role-based access permissions
- Multi-factor authentication requirements
- Regular access reviews and audit logging
- Secure credential management

7.2 Retention Periods

- Client data: Retained for the duration of the business relationship plus 5 years for legal and tax purposes.
- Prospect data: Retained for 2 years from last contact or interaction.
- Marketing data: Reviewed and validated every 12 months.
- Database contacts: Reviewed and updated every 6 months to ensure accuracy.
- Financial records: Retained for 7 years as required by South African tax law.
- Website usage data: Retained for 13 months.

7.3 Data Disposal

When data is no longer needed according to our retention schedule, it is securely deleted or anonymized using industry-standard methods.

8. DATA BREACH NOTIFICATION

8.1 Internal Procedures

We maintain comprehensive data breach detection and response procedures. All potential breaches are immediately escalated to the Information Officer.

8.2 Cloud Provider Breaches

In the event of a security incident affecting our cloud service providers:

- We will coordinate with the provider to assess the impact on our data
- We maintain incident response plans specifically for cloud-based data storage
- Our Information Officer will monitor the provider's breach notifications
- We will independently evaluate whether notification obligations are triggered

8.3 Notification Timeframes

- To Regulatory Authorities: We will notify the Information Regulator within 72 hours of becoming aware of a breach that risks the rights and freedoms of individuals.
- To Affected Individuals: Where a breach is likely to result in high risk to rights and freedoms, we will notify affected individuals without undue delay.
- To Clients: Where the breach affects client data or services, we will notify affected clients within 24 hours.

8.4 Breach Information

Notifications will include the nature of the breach, categories and approximate number of records concerned, likely consequences, measures taken, and contact information for further inquiries.

9. DATA SHARING & THIRD PARTIES

We do not sell or rent Personal Information. However, we may share data with:

- Cloud Service Providers – Google Workspace and other enterprise cloud services that store and process our aggregated data.
- Service Providers – Payment processors, CRM systems, email marketing platforms, and other operational tools.
- Sales Agents – Authorized representatives who conduct outreach activities on our behalf.
- AI Service Providers – Partners who provide AI-driven analytics and messaging optimization.
- Legal Authorities – When required by law or regulatory enforcement.
- Business Transfers – In case of mergers, acquisitions, or business restructuring.

All third-party partners and agents must adhere to strict data protection obligations through appropriate contractual measures. For cloud service providers, we implement data processing agreements that include:

- Clearly defined data handling responsibilities
- Confidentiality commitments
- Security requirements
- Obligations to assist with data subject rights requests
- Breach notification requirements

10. DATA SUBJECT RIGHTS

Under POPIA & GDPR, Data Subjects have the right to:

- Access Personal Information
- Request Data Correction or Deletion
- Withdraw Consent at Any Time
- Object to Processing for Marketing Purposes
- Restrict Processing in Certain Circumstances
- Request Data Portability (GDPR-specific)
- Not be Subject to Automated Decision-Making (certain circumstances)

10.1 How to Exercise Your Rights

- Submit requests via email to info@plera.co or through our website form.
- Provide sufficient information to verify your identity.
- Specify which right(s) you wish to exercise.

10.2 Response Timeframes

- We will acknowledge receipt of your request within 3 business days.
- We will respond substantively to your request within 21 calendar days.
- Complex requests may require an additional 21 days, in which case we will notify you.

11. CHILDREN'S DATA

We do not knowingly collect or process personal information from individuals under the age of 18. If we become aware that we have inadvertently collected personal information from a minor, we will promptly delete such information from our records.

10. DATA SUBJECT RIGHTS

Under POPIA & GDPR, Data Subjects have the right to:

- Access Personal Information
- Request Data Correction or Deletion
- Withdraw Consent at Any Time
- Object to Processing for Marketing Purposes
- Restrict Processing in Certain Circumstances
- Request Data Portability (GDPR-specific)
- Not be Subject to Automated Decision-Making (certain circumstances)

10.1 How to Exercise Your Rights

- Submit requests via email to info@plera.co or through our website form.
- Provide sufficient information to verify your identity.
- Specify which right(s) you wish to exercise.

10.2 Response Timeframes

- We will acknowledge receipt of your request within 3 business days.
- We will respond substantively to your request within 21 calendar days.
- Complex requests may require an additional 21 days, in which case we will notify you.

11. CHILDREN'S DATA

We do not knowingly collect or process personal information from individuals under the age of 18. If we become aware that we have inadvertently collected personal information from a minor, we will promptly delete such information from our records.

12. INTERNATIONAL DATA TRANSFERS AND CLIENTS

12.1 Cross-Border Data Transfers

We may transfer data internationally to service providers located outside of South Africa. In such cases, we ensure adequate data protection measures through:

- Standard Contractual Clauses approved by the European Commission
- Adequacy decisions where applicable
- Binding Corporate Rules for intra-group transfers
- Other appropriate safeguards as required by POPIA and GDPR

12.2 International Clients

This Privacy Policy applies to all our clients globally, with the following additional provisions:

12.2.1 Applicable Laws

- While we are primarily governed by South African law (POPIA), we strive to comply with major international data protection regulations including GDPR (Europe), CCPA/CPRA (California), PIPEDA (Canada), and others as applicable.
- Where conflicts arise between legal requirements, we will apply the higher standard of protection.

12.2.2 Regional Representatives

- As we expand into EU and UK markets, we are establishing arrangements with qualified local representatives in accordance with GDPR and UK GDPR requirements. We take a phased approach to representation, prioritizing jurisdictions where we have active client relationships while working toward comprehensive coverage. Until a permanent representative is appointed for a specific region, all data protection inquiries can be directed to our Information Officer.
- For other regions requiring local representatives, we take a similar approach of appointing qualified representatives in compliance with local regulations as our business develops in those areas.

12.2.3 Regional-Specific Rights
Depending on your jurisdiction, you may have additional rights beyond those outlined in Section 10, including:

- California Residents: Rights under CCPA/CPRA including the right to opt-out of "sales" of personal information and the right to equal service and pricing.
- Canadian Residents: Rights under PIPEDA including challenging compliance.
- Brazilian Residents: Rights under LGPD including the right to information about public and private data sharing.

12.2.4 Legal Basis for International Processing
For international data processing, we rely on:

- Performance of contract with international clients
- Legitimate interests for business development
- Explicit consent where required by local law
- Legal obligations applicable in the relevant jurisdiction

13. COOKIES & TRACKING TECHNOLOGIES
We use cookies and similar tracking technologies for:

- Website functionality and security
- Analytics and performance tracking
- Targeted advertising (only with consent)

Users can manage cookie preferences via their browser settings or our cookie management tool.

14. SALES AGENT TERMS

14.1 Agent Data Handling

- All sales agents must adhere to this Privacy Policy.
- Agents receive training on appropriate data handling practices.
- Agents may only access and use data necessary for their specific role.
- Agent activities are logged and monitored for compliance.

14.2 AI-Assisted Communications

- Our proprietary AI systems may assist agents in crafting personalized communications.
- These systems operate under strict protocols to ensure compliance with data protection laws.
- Recipients of AI-assisted communications retain all rights outlined in this policy.

15. REGULATORY AUTHORITY

The Information Regulator (South Africa) is the supervisory authority for data protection matters:
Information Regulator (South Africa)
JD House, 27 Stiemens Street
Braamfontein, Johannesburg, 2001
Email: inforeg@justice.gov.za
Website: https://www.justice.gov.za/inforeg/

16. CHANGES TO THIS POLICY

We reserve the right to update this policy. Any significant changes will be communicated via our website or email at least 14 days before implementation.

17. GOVERNING LAW AND JURISDICTION

17.1 Primary Governing Law
This Privacy Policy shall be governed by and construed in accordance with the laws of the Republic of South Africa, particularly the Protection of Personal Information Act (POPIA).
17.2 Dispute Resolution
Any dispute arising out of or in connection with this Privacy Policy, including any question regarding its existence, validity, or termination, shall be referred to and finally resolved as follows:

- For South African clients: By the courts of South Africa.
- For international clients: Initially through good faith negotiation. If unresolved within 30 days, disputes will be settled according to the laws of the Republic of South Africa, with due consideration to mandatory provisions of the client's local data protection laws that cannot be derogated from by agreement.

17.3 Non-Exclusive Jurisdiction
Nothing in this Privacy Policy limits the right of a Data Subject to:

- Lodge a complaint with their local data protection authority
- Seek recourse through their local courts if mandatory local laws so provide
-

18. CONTACT INFORMATION

For questions or concerns regarding this policy, contact us at:
Plera (Pty) Ltd
Email: info@plera.co
Physical Address:
708 NEW BOSTON
85 VOORTREKKER ROAD
BELLVILLE
WESTERN CAPE
7530