PRIVACY POLICY

CHRONOLOGIC SOLUTIONS (PTY) LTD
Registration Number: 2003/003093/07

Date of Compilation: March 2014
Last Updated: October 2025

TABLE OF CONTENTS

1. INTRODUCTION AND DEFINITIONS

1.1 About This Policy

Chronologic Solutions (Pty) Ltd ("**Chronologic**", "**we**", "**us**", or "**our**") is committed to protecting and respecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your personal information when you:

- Visit our website at https://chronologic.co.za ("**the Website**")
- Use our IT services and solutions
- Communicate with us
- Interact with our marketing materials

1.2 Legal Compliance

We comply with all applicable privacy and data protection laws, including:

- The Constitution of the Republic of South Africa, 1996
- The Protection of Personal Information Act, 4 of 2013 ("**POPIA**")
- The Promotion of Access to Information Act, 2 of 2000 ("**PAIA**")
- The Electronic Communications and Transactions Act, 25 of 2002
- The Cybercrimes Act, 19 of 2020

1.3 Definitions

For purposes of this Privacy Policy:

- "**Personal Information**" means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, as defined in POPIA
- "**Processing**" means any operation or activity concerning personal information, including collection, receipt, recording, organization, collation, storage, updating, modification, retrieval, alteration, consultation, use, dissemination, merging, linking, restriction, degradation, erasure, or destruction of information
- "**You**" or "**User**" means the person accessing the Website or using our services, or on whose behalf the Website is accessed or services are used
- "**Services**" means all IT solutions, managed services, cybersecurity services, cloud services, IT advisory services, and related offerings provided by Chronologic

1.4 Acceptance of This Policy

By accessing our Website or using our Services, you acknowledge that you have read, understood, and agree to be bound by this Privacy Policy. If you do not agree with this Privacy Policy, please do not use our Website or Services.

1.5 Relationship with Other Documents

This Privacy Policy should be read together with:

- Our Website Terms of Use (available on the Website)
- Our PAIA Manual (available at https://chronologic.co.za)
- Any service agreements or contracts between you and Chronologic
- Our Cookie Policy (see Section 7 below)

2. INFORMATION OFFICER DETAILS

2.1 Information Officer

In accordance with POPIA and PAIA, we have appointed an Information Officer who is responsible for ensuring compliance with data protection legislation and handling all privacy-related queries and requests.

Information Officer:
Name: Natasha Singh
Title: Compliance Manager
Email: info@chronologic.co.za
Telephone: +27 10 591 8105
Physical Address: Optimum House, Epson Downs Business Park, Sloane Street, Bryanston, 2195
Postal Address: Optimum House, Epson Downs Business Park, Sloane Street, Bryanston, 2195

2.2 Contacting the Information Officer

You may contact our Information Officer for:

- Questions about this Privacy Policy
- Requests to access, correct, or delete your personal information
- Complaints about our handling of your personal information
- Requests to withdraw consent for processing

- Objections to processing of your personal information
- Any other privacy-related concerns

We will respond to your query within a reasonable time, and no later than 30 days from receipt.

3. INFORMATION WE COLLECT

We collect only the personal information that is necessary for the purposes outlined in this Privacy Policy. The information we collect includes:

3.1 Information You Provide Directly

Contact Information:

- Full name and surname
- Email address
- Telephone and mobile numbers
- Physical and postal addresses
- Company name and registration details (for business clients)
- Job title and department

Account Information:

- Username and password (encrypted)
- Security questions and answers
- Account preferences and settings

Service-Related Information:

- Information in service requests, support tickets, and inquiries
- Project specifications and requirements
- Technical requirements and preferences
- Feedback, surveys, and testimonials
- Communication records (emails, calls, messages)

Financial Information:

- Billing addresses

- Payment method details (processed securely by third-party payment processors)
- Purchase history and invoices
- Banking details for payments (where applicable)

Employment Information (if you apply for a position with us):

- CV/resume and cover letter
- Employment history and references
- Qualifications and certifications
- Identity document details

3.2 Information We Collect Automatically

Website Usage Information:

- IP address
- Browser type and version
- Operating system
- Device information (type, model, identifiers)
- Pages visited and time spent on pages
- Links clicked
- Referring website/source
- Date and time of visits
- Language preferences

Technical and System Information (when providing Services):

- IT environment configurations
- System access logs
- Network information and diagrams
- Software and hardware inventories
- Performance metrics and analytics
- Security incident logs
- Backup and recovery data

Cookies and Tracking Data:

- Cookie identifiers
- Session data
- Analytics data
- Marketing tracking data

(See Section 7 for detailed information about cookies)

3.3 Information from Third Parties

We may receive information about you from:

- Our business partners and resellers
- Service providers and subcontractors
- Public databases and registers
- Social media platforms (if you interact with us there)
- References and background check providers (for employment)

3.4 Sensitive Personal Information

We do not generally collect sensitive personal information (such as health data, religious beliefs, criminal records, etc.) unless specifically required for employment purposes or with your explicit consent and where permitted by law.

4. HOW WE COLLECT INFORMATION

We collect your personal information through various channels:

4.1 Direct Collection

- When you fill out forms on our Website
- When you contact us via email, phone, or in person
- When you sign up for newsletters or marketing materials
- When you request a quote or proposal
- When you enter into a service agreement with us
- When you participate in surveys or provide feedback
- When you apply for employment

4.2 Automatic Collection

- Through cookies and similar technologies on our Website
- Through system monitoring and logging when providing Services
- Through analytics tools and services
- Through security monitoring systems

4.3 Third-Party Sources

- From our business partners and affiliates
- From publicly available sources
- From service providers acting on our behalf

5. HOW WE USE YOUR INFORMATION

We process your personal information for the following purposes:

5.1 Service Delivery and Management

- To provide our IT solutions and managed services
- To set up and manage user accounts
- To process transactions and manage billing
- To provide technical support and troubleshooting
- To manage IT environments and infrastructure
- To perform system monitoring and maintenance
- To implement cybersecurity measures
- To manage cloud services and hosting
- To ensure service quality and performance

5.2 Communication

- To respond to your inquiries and requests
- To send service-related notifications and updates
- To provide customer support
- To send invoices and payment reminders

- To notify you of changes to our Services or policies

5.3 Website Functionality

- To enable efficient use of the Website
- To improve Website performance and user experience
- To personalize your Website experience
- To remember your preferences and settings
- To process online transactions

5.4 Marketing and Business Development

- To send newsletters and promotional materials (with your consent)
- To inform you about new services and offerings
- To conduct market research and surveys
- To analyse customer preferences and trends
- To improve our Services and develop new offerings

5.5 Legal and Compliance

- To comply with legal obligations and regulatory requirements
- To enforce our terms and conditions
- To protect our legal rights and interests
- To prevent fraud and unauthorized access
- To detect and respond to security incidents
- To maintain records as required by law

5.6 Internal Operations

- For business administration and management
- For financial reporting and accounting
- For internal audits and risk management
- For training and quality assurance
- For business continuity and disaster recovery

5.7 Employment

- To process job applications
- To conduct background checks (with consent)
- To manage employee records and benefits
- To comply with employment legislation

6. LEGAL BASIS FOR PROCESSING

Under POPIA, we must have a lawful basis for processing your personal information. We process your personal information based on one or more of the following:

6.1 Consent

Where you have given us clear, voluntary, and informed consent to process your personal information for specific purposes (e.g., marketing communications, cookies).

6.2 Contractual Necessity

Where processing is necessary to perform our contractual obligations to you or to take steps at your request before entering into a contract (e.g., providing Services, processing payments).

6.3 Legal Obligation

Where we are required by law to process your personal information (e.g., tax compliance, regulatory reporting, record retention requirements).

6.4 Legitimate Interests

Where processing is necessary for our legitimate business interests or those of a third party, provided these interests do not override your fundamental rights (e.g., fraud prevention, network security, business analytics, internal administration).

6.5 Protection of Vital Interests

Where processing is necessary to protect your vital interests or those of another person (e.g., medical emergencies).

You have the right to object to processing based on legitimate interests. Please contact our Information Officer to exercise this right.

7. COOKIES AND TRACKING TECHNOLOGIES

7.1 What Are Cookies?

Cookies are small text files that are placed on your device when you visit our Website. They help us provide you with a better experience by remembering your preferences and understanding how you use our Website.

7.2 Types of Cookies We Use

Essential Cookies (Strictly Necessary)

- Required for the Website to function properly
- Enable basic functions like page navigation and access to secure areas
- Cannot be disabled without affecting Website functionality
- No consent required as they are essential for service delivery

Performance/Analytics Cookies

- Collect information about how visitors use our Website
- Help us understand which pages are most popular
- Allow us to improve Website performance
- Examples: Google Analytics, website traffic analysis
- Require consent

Functionality Cookies

- Remember your preferences and choices
- Provide enhanced features and personalization
- May remember your login details (if you choose)
- Require consent

Marketing/Advertising Cookies

- Track your browsing habits across websites
- Used to deliver relevant advertisements
- Help us measure the effectiveness of our marketing campaigns
- May be set by third-party advertising networks
- Require consent

7.3 Third-Party Cookies

Some cookies are placed by third-party services that appear on our Website, such as:

- Google Analytics (website analytics)
- Social media plugins (LinkedIn, Facebook, Twitter)
- Marketing and advertising platforms
- Live chat services

These third parties have their own privacy policies, and we have no control over their cookies.

7.4 Managing Cookies

Browser Settings: You can control and manage cookies through your browser settings. Most browsers allow you to:

- Block all cookies
- Block third-party cookies
- Delete cookies after you close your browser
- Accept cookies from specific websites only

Please note that blocking or deleting cookies may impact your experience on our Website and may prevent certain features from working properly.

Cookie Consent Tool: When you first visit our Website, you will see a cookie consent banner allowing you to accept or reject non-essential cookies. You can change your preferences at any time by clicking the "Cookie Settings" link in our Website footer.

7.5 Other Tracking Technologies

We may also use:

- **Web beacons/pixels** - Small graphic images used to track email opens and Website activity
- **Session storage** - Temporary storage of information during your browsing session
- **Local storage** - Storage of preferences and settings on your device

7.6 Do Not Track Signals

Some browsers have a "Do Not Track" feature. Currently, there is no industry standard for responding to these signals. Our Website does not respond to Do Not Track requests, but you can control cookies as described above.

8. HOW WE SHARE YOUR INFORMATION

We do not sell, rent, or trade your personal information to third parties. However, we may share your information with the following categories of recipients:

8.1 Service Providers and Business Partners

We share personal information with trusted third-party service providers who assist us in operating our business and delivering Services, including:

IT Service Providers:

- Cloud hosting and infrastructure providers
- Data backup and disaster recovery services
- Software vendors and technology partners
- Cybersecurity service providers
- System monitoring and management tools

Business Service Providers:

- Payment processors and merchant services
- Accounting and bookkeeping services
- Legal advisors and auditors
- Insurance providers
- Debt collection agencies (where applicable)

Marketing Service Providers:

- Email marketing platforms
- Marketing analytics services
- Advertising networks
- Customer relationship management (CRM) systems

All service providers are bound by confidentiality agreements and are only permitted to use your personal information as necessary to provide services to us. They may not use your information for their own purposes.

8.2 Business Partners and Resellers

We may share information with authorized resellers, technology partners, and business associates where necessary to deliver Services to you or where you have engaged with us through such partners.

8.3 Legal and Regulatory Authorities

We may disclose your personal information to:

- Law enforcement agencies, courts, or regulatory bodies when required by law
- Government agencies for tax, compliance, or regulatory purposes (e.g., SARS)
- Legal advisors in connection with legal proceedings

8.4 Corporate Transactions

If we undergo a merger, acquisition, reorganization, or sale of assets, your personal information may be transferred to the successor entity, subject to confidentiality obligations and notification to affected individuals.

8.5 With Your Consent

We may share your information with other third parties where you have provided explicit consent for us to do so.

8.6 Protection of Rights

We may disclose personal information where we believe it is necessary to:

- Protect our legal rights and interests
- Enforce our terms and conditions
- Prevent fraud or security threats
- Protect the safety and security of our employees, clients, or the public
- Protect against misuse or unauthorized use of our Services

9. TRANSBORDER FLOW OF PERSONAL INFORMATION

9.1 International Data Transfers

Due to the nature of our business and the use of cloud services and international technology providers, your personal information may be transferred to, stored in, or processed in countries outside the Republic of South Africa.

Reasons for international transfers include:

- Cloud hosting and data storage services
- Software-as-a-Service (SaaS) providers
- Technical support from international vendors
- Backup and disaster recovery services
- Email and communication platforms
- Marketing and analytics tools

9.2 Countries and Regions

Personal information may be transferred to recipients in the following regions:

- European Union (EU) member states
- United States of America
- United Kingdom
- Other countries where our service providers operate

9.3 Safeguards for International Transfers

We ensure that international transfers of personal information are protected by appropriate safeguards, including:

- **Adequacy determinations** - Transferring to countries that the Information Regulator or equivalent authority recognizes as providing adequate data protection
- **Standard contractual clauses** - Using legally approved contract templates that require recipients to protect your information
- **Binding corporate rules** - Where service providers have internal policies approved by data protection authorities
- **Consent** - Obtaining your explicit consent for specific transfers where required
- **Necessity** - Where the transfer is necessary for the performance of a contract or implementation of pre-contractual measures

9.4 Your Rights

You have the right to:

- Request information about international transfers of your personal information
- Object to specific international transfers (subject to legal and contractual limitations)
- Withdraw consent for international transfers (where consent is the legal basis)

Contact our Information Officer to exercise these rights or for more information about our international data transfers.

10. DATA SECURITY

10.1 Our Commitment to Security

We take the security of your personal information seriously and have implemented appropriate technical and organizational measures to protect it against unauthorized access, loss, destruction, alteration, or disclosure.

10.2 Technical Security Measures

Network and Infrastructure Security:

- Enterprise-grade firewalls and intrusion detection/prevention systems
- Network segmentation and access controls
- Regular security patching and updates
- Vulnerability scanning and penetration testing
- DDoS protection and mitigation
- 24/7 security monitoring and logging

Data Protection:

- Encryption of data in transit (TLS/SSL)
- Encryption of data at rest for sensitive information
- Secure backup systems with encryption
- Data loss prevention (DLP) tools
- Secure deletion and destruction procedures

Access Control:

- Multi-factor authentication (MFA) for system access
- Role-based access controls (RBAC)
- Principle of least privilege
- Strong password policies
- Regular access reviews and audits
- Immediate revocation of access for departed personnel

Application Security:

- Secure coding practices
- Regular security updates and patches
- Web application firewalls (WAF)
- Input validation and sanitization
- Secure session management

10.3 Organizational Security Measures

Policies and Procedures:

- Comprehensive information security policies
- Data classification and handling procedures
- Incident response and management procedures
- Business continuity and disaster recovery plans
- Acceptable use policies
- Clean desk and clear screen policies

Personnel Security:

- Background checks for employees with access to sensitive information
- Confidentiality and non-disclosure agreements for all staff
- Regular security awareness training
- Security responsibilities in job descriptions
- Disciplinary procedures for security violations

Physical Security:

- Controlled access to offices and data centers
- Security systems (alarms, CCTV)
- Visitor management procedures
- Secure storage for physical records
- Secure disposal of documents containing personal information

Vendor Management:

- Due diligence on third-party service providers
- Contractual security requirements
- Regular vendor security assessments
- Service level agreements (SLAs) with security provisions

10.4 Limitations

While we implement industry-leading security measures, no method of transmission over the Internet or electronic storage is 100% secure. We cannot guarantee absolute security, but we will:

- Continuously monitor and improve our security measures
- Respond promptly to security incidents
- Notify affected individuals of data breaches as required by law
- Investigate and remediate security vulnerabilities

10.5 Your Responsibilities

You can help protect your personal information by:

- Keeping your login credentials confidential
- Using strong, unique passwords
- Enabling multi-factor authentication where available
- Not sharing your account with others
- Being cautious of phishing emails and suspicious communications
- Keeping your devices and software updated
- Reporting suspected security incidents to us immediately

11. DATA RETENTION

11.1 Retention Principles

We retain your personal information only for as long as necessary to fulfil the purposes for which it was collected and to comply with legal, regulatory, and business requirements.

11.2 Retention Periods

General Business Records:

- Client contracts and agreements: Duration of contract + 7 years
- Financial records (invoices, payments): 5 years (as required by tax legislation)
- Correspondence and communications: 2-5 years depending on nature

IT Service Records:

- Technical support tickets: 3 years
- System logs and monitoring data: 6-12 months (longer if security incident related)
- IT environment configurations: Duration of service + 1 year
- Security incident records: 5 years

Employee Records:

- Personnel files: Duration of employment + 5 years
- Payroll records: 3-5 years (as required by law)
- Employment applications (unsuccessful): 1 year

Website and Marketing:

- Website analytics data: 12-26 months
- Marketing communications preferences: Until consent withdrawn + 1 year
- Cookie data: As specified in cookie settings (typically 12-24 months)

Legal and Compliance:

- Legal documents and opinions: 10 years
- Regulatory compliance records: As required by specific legislation
- Audit reports: 7 years

11.3 Exceptions to Retention Periods

We may retain personal information beyond the standard retention periods where:

- Required by law or court order
- Necessary for ongoing legal proceedings or investigations
- Required to protect our legal rights or defend against claims
- Necessary for historical, statistical, or research purposes (in anonymized form)
- You have specifically requested that we retain your information

11.4 Secure Deletion

When personal information is no longer required, we securely delete or anonymize it using appropriate methods:

- Secure overwriting or wiping of electronic data
- Destruction of physical documents (shredding, pulping)
- Secure disposal by certified vendors
- Verification of deletion/destruction

11.5 Anonymization

Where possible, we may retain data in anonymized form for statistical, analytical, or reporting purposes. Anonymized data cannot be linked back to you and is not considered personal information under POPIA.

12. YOUR PRIVACY RIGHTS

Under POPIA and other applicable legislation, you have the following rights regarding your personal information:

12.1 Right to Access

You have the right to:

- Request confirmation of whether we hold personal information about you
- Request access to your personal information
- Request details about how we process your personal information
- Request a copy of your personal information

How to exercise: Submit a request to our Information Officer using the PAIA request form (available in our PAIA Manual at https://chronologic.co.za).

Timeframe: We will respond within 30 days of receiving your request.

Fees: A prescribed fee may apply (see our PAIA Manual for details). Access to your own personal information is generally free, but we may charge for additional copies or administrative costs.

12.2 Right to Correction

You have the right to request correction, deletion, or updating of inaccurate, irrelevant, excessive, out-of-date, incomplete, or misleading personal information.

How to exercise: Contact our Information Officer with details of the information requiring correction and supporting evidence where applicable.

Timeframe: We will action your request within a reasonable time, generally within 30 days.

12.3 Right to Deletion (Right to be Forgotten)

You have the right to request deletion of your personal information where:

- The information is no longer necessary for the purpose for which it was collected
- You withdraw consent (where consent was the basis for processing)
- You object to processing and we have no overriding legitimate grounds
- The information has been processed unlawfully
- Deletion is required to comply with legal obligations

Limitations: We may be unable to delete your information if retention is required by law or necessary for legal claims, compliance, or other legitimate purposes.

How to exercise: Submit a written request to our Information Officer with reasons for the deletion request.

12.4 Right to Object

You have the right to object to the processing of your personal information on reasonable grounds relating to your particular situation, unless legislation provides for such processing.

Specifically, you may object to:

- Processing for direct marketing purposes (at any time)

- Processing based on legitimate interests

How to exercise: Submit an objection to our Information Officer explaining your grounds for objection.

Effect: If you object to marketing, we will cease marketing communications immediately. For other objections, we will assess whether we have compelling legitimate grounds to continue processing.

12.5 Right to Restrict Processing

In certain circumstances, you may request that we restrict how we use your personal information while we:

- Verify the accuracy of information you have disputed
- Assess your objection to processing
- Retain information for your legal claims even though we no longer need it

12.6 Right to Data Portability

Where technically feasible and where processing is based on consent or contract and carried out by automated means, you have the right to:

- Receive your personal information in a structured, commonly used, machine-readable format
- Transmit that information to another organization

Limitations: This right applies only to information you provided to us and does not apply to all types of processing.

12.7 Right to Withdraw Consent

Where we process your personal information based on your consent, you have the right to withdraw that consent at any time.

How to exercise: Contact our Information Officer or use the unsubscribe link in marketing communications.

Effect: Withdrawal of consent does not affect the lawfulness of processing before withdrawal. We may continue processing based on other lawful grounds.

12.8 Right to Lodge a Complaint

If you believe we have processed your personal information unlawfully or violated your privacy rights, you have the right to:

- Lodge a complaint with our Information Officer
- Lodge a complaint with the Information Regulator (see Section 20 for contact details)
- Approach a court of competent jurisdiction

12.9 Exercising Your Rights

To exercise any of these rights:

Contact our Information Officer:

- Email: info@chronologic.co.za
- Telephone: +27 10 591 8105
- Post: Natasha Singh, Compliance Manager, Optimum House, Epson Downs Business Park, Sloane Street, Bryanston, 2195

What we need from you:

- Proof of identity (copy of ID or other acceptable identification)
- Clear description of your request
- Specific information about which rights you wish to exercise
- Any relevant supporting information

Our response:

- We will acknowledge your request within 5 business days
- We will respond substantively within 30 days (or notify you if we need additional time)
- We will explain any reasons for refusing a request
- We will inform you of your right to complain to the Information Regulator

12.10 Fees for Exercising Rights

Generally, we do not charge a fee for processing requests to exercise your rights. However, we may charge a reasonable administrative fee if:

- Your request is manifestly unfounded or excessive
- You request additional copies of information already provided

We will inform you of any applicable fees before processing your request.

13. MARKETING COMMUNICATIONS

13.1 Consent for Marketing

We will only send you marketing communications if:

- You have given us explicit, voluntary, and informed consent to do so, or
- You are an existing client and the marketing relates to similar services to those you use, and you have not opted out

Marketing communications may include:

- Newsletters and updates
- Information about new services and solutions
- Promotional offers and special pricing
- Invitations to events, webinars, and training
- Industry news and insights
- Case studies and success stories

13.2 How We Obtain Consent

We obtain consent for marketing through:

- Opt-in checkboxes on Website forms (not pre-ticked)
- Explicit requests to subscribe to newsletters
- Verbal consent during sales calls (documented)
- Written consent in contracts (where separate from service provision)

Consent for marketing is always separate from consent to receive service-related communications, which we may send as part of our contractual relationship.

13.3 What We Send

Our marketing communications may include:

- Email newsletters (periodic)
- Product/service announcements
- Educational content and resources
- Event invitations
- Customer satisfaction surveys

13.4 Tracking Marketing Effectiveness

We may track whether you:

- Open our marketing emails
- Click on links within emails
- Visit specific pages on our Website after receiving marketing
- Engage with our content on social media

This helps us improve the relevance and quality of our communications.

13.5 Opting Out (Unsubscribing)

You can opt out of marketing communications at any time by:

Email unsubscribe:

- Click the "Unsubscribe" link at the bottom of any marketing email
- You will be removed from our marketing list immediately (allow up to 5 business days for processing)

Contact us directly:

- Email: info@chronologic.co.za with "Unsubscribe" in the subject line
- Telephone: +27 10 591 8105
- Written request to our postal address

Update preferences:

- We may offer preference centres where you can choose which types of communications you wish to receive

13.6 Effect of Opting Out

If you opt out of marketing:

- We will stop sending you marketing communications
- You will continue to receive essential service-related communications (invoices, service updates, security notifications, etc.)
- Your personal information will remain in our database for business purposes unless you request deletion (subject to our legal obligations to retain certain information)

- We will retain your "unsubscribe" preference to ensure we don't contact you again for marketing purposes

13.7 Third-Party Marketing

We do not sell or rent our mailing lists to third parties. We will never share your information with third parties for their own marketing purposes without your explicit consent.

14. CHILDREN'S PRIVACY

14.1 Age Restriction

Our Website and Services are not intended for, and we do not knowingly collect personal information from, children under the age of 18 years ("**minors**").

14.2 Parental Consent

If we need to process personal information of a minor (for example, if a minor applies for employment or internship with parental consent), we will:

- Obtain verifiable consent from a parent or legal guardian before collecting the information
- Only collect information necessary for the specific purpose
- Take extra care to protect the minor's personal information

14.3 If We Discover We Have Collected Children's Information

If we become aware that we have inadvertently collected personal information from a minor without proper parental consent, we will:

- Delete the information as soon as reasonably possible
- Not use the information for any purpose
- Not disclose the information to third parties

14.4 Parents and Guardians

If you are a parent or guardian and believe your child has provided us with personal information without your consent, please contact our Information Officer immediately at info@chronologic.co.za. We will investigate and take appropriate action.

15. THIRD-PARTY WEBSITES AND SERVICES

15.1 Links to Third-Party Websites

Our Website may contain links to third-party websites, applications, or services that are not operated or controlled by Chronologic, including:

- Technology vendor websites
- Partner and reseller websites
- Social media platforms
- Industry resources and publications
- Customer websites (where we provide services)

15.2 No Responsibility for Third Parties

We are not responsible for:

- The privacy practices of third-party websites or services
- The content, accuracy, or reliability of third-party sites
- Any loss or damage resulting from your use of third-party sites

15.3 Third-Party Privacy Policies

When you click on a link to a third-party website:

- You will leave our Website
- You will be subject to that third party's privacy policy and terms of use
- We encourage you to review the privacy policies of any third-party sites you visit

15.4 Social Media

Our Website may include social media features and widgets (such as LinkedIn, Facebook, Twitter share buttons) that:

- Are hosted by third-party social media platforms
- May collect information about your visit to our Website
- May set cookies to enable the feature to function properly
- Are governed by the privacy policies of the respective social media platforms

15.5 Third-Party Service Providers

While we use third-party service providers to help us deliver our Services (as described in Section 8), these providers are bound by contractual obligations to protect your information and use it only as directed by us.

16. AUTOMATED DECISION-MAKING

16.1 Use of Automated Processing

We may use automated processing, including profiling, in limited circumstances:

Website Personalization:

- Displaying relevant content based on your browsing behaviour
- Customizing user experience based on preferences
- Recommending services based on previous interactions

Fraud Prevention:

- Automated checks for fraudulent transactions
- Risk assessment for security purposes
- Spam and bot detection

Marketing Optimization:

- Segmentation of marketing audiences
- Targeting of relevant advertisements
- A/B testing of marketing content

16.2 Significant Automated Decisions

We do not make significant decisions that produce legal effects or similarly significantly affect you based solely on automated processing without human involvement.
Examples of decisions we do NOT make automatically include:

- Decisions to enter into or terminate contracts
- Decisions affecting your credit rating
- Employment decisions
- Pricing decisions (except standard published pricing)

16.3 Your Rights

If we use automated decision-making that significantly affects you, you have the right to:

- Be informed about the logic involved
- Request human intervention and review
- Express your point of view
- Contest the decision

Contact our Information Officer to exercise these rights.

17. DATA BREACH NOTIFICATION

17.1 Our Commitment

We take data security seriously and have implemented measures to prevent data breaches. However, in the event that a data breach occurs, we are committed to handling it responsibly and in compliance with POPIA.

17.2 What is a Data Breach?

A data breach means unauthorized access to, or acquisition, loss of, damage to, or unauthorized destruction of personal information that compromises the confidentiality, integrity, or availability of that information.

Examples include:

- Unauthorized access to our systems or databases
- Theft or loss of devices containing personal information
- Ransomware or malware attacks
- Accidental disclosure of personal information
- Loss or theft of physical documents

17.3 Data Breach Response Procedure

If we discover or are notified of a data breach, we will:

Immediate Response (within 24 hours):

- Contain and secure the breach to prevent further unauthorized access
- Assess the nature and extent of the breach

- Activate our incident response team
- Preserve evidence for investigation

Investigation (within 72 hours):

- Determine what personal information was affected
- Identify affected individuals and data subjects
- Assess the potential impact and risks to affected individuals
- Determine the cause and how the breach occurred
- Implement remedial measures

Notification (as soon as reasonably possible):

- Notify the Information Regulator without undue delay where the breach is likely to pose a risk of harm to data subjects
- Notify affected individuals where the breach poses a risk of serious harm
- Provide clear information about the breach and recommended actions

17.4 What We Will Tell You

If we notify you of a data breach, we will provide:

- A description of the breach and how it occurred
- The type of personal information affected
- The potential consequences and risks
- Measures we have taken or will take to address the breach
- Recommendations for you to protect yourself
- Contact details for further information and assistance
- Your right to lodge a complaint with the Information Regulator

17.5 Notification to the Information Regulator

We will notify the Information Regulator of any breach that poses a risk of harm, providing:

- Description of the breach
- Description of affected personal information
- Number of affected data subjects

- Potential consequences
- Measures taken or proposed to address the breach
- Recommendations to mitigate adverse effects

17.6 When We May Not Notify You

We may not be required to notify you if:

- The breach poses no risk of harm to you
- We have implemented measures to reduce the risk to an acceptable level
- The information was already publicly available
- Notification would impede a criminal investigation (but we will notify once permitted)

17.7 Your Responsibilities

If you suspect a data breach or security incident:

- Notify us immediately at info@chronologic.co.za
- Change your passwords if you believe your account may be compromised
- Monitor your accounts for suspicious activity
- Follow any additional instructions we provide

17.8 Data Breach Register

We maintain an internal register of all data breaches (significant or minor) for monitoring, compliance, and continuous improvement purposes.

18. CHANGES TO THIS PRIVACY POLICY

18.1 Right to Modify

We reserve the right to modify, update, or replace this Privacy Policy at any time to:

- Reflect changes in our business practices
- Comply with new legal or regulatory requirements
- Improve clarity and transparency
- Add new services or features
- Address feedback from users or regulators

18.2 How We Notify You of Changes

Significant Changes: If we make material changes that affect how we collect, use, or share your personal information, we will notify you by:

- Email notification to your registered email address (at least 30 days before changes take effect)
- Prominent notice on our Website homepage
- Pop-up notification when you next visit our Website

Minor Changes: For non-material changes (such as clarifications, corrections, or formatting), we will:

- Update the "Last Updated" date at the top of this Privacy Policy
- Post the updated policy on our Website

18.3 Reviewing Changes

We encourage you to:

- Review this Privacy Policy periodically
- Check the "Last Updated" date to see when it was last modified
- Contact our Information Officer if you have questions about changes

18.4 Acceptance of Changes

By continuing to use our Website or Services after changes take effect, you acknowledge and accept the updated Privacy Policy. If you do not agree with the changes, you should:

- Stop using our Website and Services
- Contact us to close your account or terminate services (subject to contractual obligations)
- Exercise your right to have your personal information deleted (subject to legal retention requirements)

18.5 Version History

We maintain a version history of this Privacy Policy. Previous versions are available upon request to our Information Officer.

19. CONTACT INFORMATION AND COMPLAINTS

19.1 Privacy Questions and Requests

For any questions, concerns, or requests regarding this Privacy Policy or our processing of your personal information, please contact our Information Officer:

Natasha Singh, Compliance Manager
Chronologic Solutions (Pty) Ltd
Email: info@chronologic.co.za
Telephone: +27 10 591 8105
Physical Address: Optimum House, Epson Downs Business Park, Sloane Street, Bryanston, 2195
Postal Address: Optimum House, Epson Downs Business Park, Sloane Street, Bryanston, 2195
Website: https://chronologic.co.za

19.2 How to Make a Complaint

If you believe we have:

- Processed your personal information unlawfully
- Violated your privacy rights
- Failed to respond adequately to your request
- Breached POPIA or other data protection laws

Step 1: Contact Our Information Officer

- Submit your complaint in writing (email or post)
- Provide details of your concern and any supporting evidence
- Include your contact information and preferred method of response

What we will do:

- Acknowledge receipt of your complaint within 5 business days
- Investigate your complaint thoroughly and impartially
- Respond substantively within 30 days
- Provide reasons for our decision
- Inform you of further steps if you remain dissatisfied

Step 2: Escalate Internally (if unresolved) If you are not satisfied with our Information Officer's response, you may escalate to:

The Board of Directors
Chronologic Solutions (Pty) Ltd
Email: info@chronologic.co.za
Postal Address: Optimum House, Epson Down Business Park, Sloane Street, Bryanston, 2195

Step 3: Lodge a Complaint with the Information Regulator If you remain dissatisfied, you have the right to lodge a complaint with the Information Regulator (see Section 20 below).

19.3 Response Timeframes

We are committed to responding to all privacy queries and complaints promptly:

- **Acknowledgment:** Within 5 business days
- **Substantive response:** Within 30 days (or notify you if more time is needed)
- **Complex matters:** Up to 60 days with notification and explanation

19.4 No Retaliation

We will not retaliate against, discriminate against, or penalize you in any way for:

- Making a privacy complaint
- Exercising your privacy rights
- Withdrawing consent for processing
- Reporting a suspected data breach

20. INFORMATION REGULATOR DETAILS

20.1 About the Information Regulator

The Information Regulator is an independent body established under POPIA to:

- Monitor and enforce compliance with POPIA and PAIA
- Handle complaints about violations of data protection laws
- Promote public awareness of data protection rights
- Issue guidance and codes of conduct

20.2 Your Right to Complain

You have the right to lodge a complaint with the Information Regulator at any time if you believe:

- We have violated your privacy rights
- We have processed your personal information unlawfully
- We have failed to comply with POPIA or PAIA
- We have not adequately responded to your complaint

You do not need to complain to us first before approaching the Information Regulator, although we encourage you to give us the opportunity to resolve your concerns.

20.3 Contact Details for the Information Regulator

The Information Regulator (South Africa)

Physical Address:
JD House
27 Stiemens Street
Braamfontein
Johannesburg, 2001
South Africa

Postal Address:
P.O. Box 31533
Braamfontein
Johannesburg, 2017
South Africa

Telephone: +27 10 023 5200
Email: inforeg@justice.gov.za
Website: https://www.justice.gov.za/inforeg/

Office Hours: Monday to Friday, 08:00 - 16:30 (excluding public holidays)

20.4 How to Lodge a Complaint

The Information Regulator provides complaint forms and guidance on their website. You will typically need to provide:

- Your contact details
- Details of the organization you are complaining about

- Description of the complaint and alleged violations
- Copies of relevant correspondence or evidence
- What outcome you are seeking

20.5 Additional Resources

The Information Regulator's website provides:

- The Guide to PAIA (in all official languages)
- Guidance on data protection rights
- Complaint procedures and forms
- Educational materials and resources
- Updates on data protection law developments

21. PAIA MANUAL

21.1 Access to Information

This Privacy Policy should be read together with our PAIA Manual, which provides detailed information about:

- Categories of records we hold
- Procedures for requesting access to records
- Grounds for refusal of access
- Fees for accessing records
- Your rights under the Promotion of Access to Information Act

21.2 Accessing Our PAIA Manual

Our PAIA Manual is available:

- On our website at https://chronologic.co.za
- At our offices during business hours (by appointment)
- From the Information Regulator's website
- Upon request to our Information Officer

21.3 Requesting Access to Your Personal Information

To request access to your personal information held by us:

- Refer to Section 12 of this Privacy Policy for procedures
- Complete the PAIA request form (Form A) available in our PAIA Manual
- Submit to our Information Officer with required identification

---

22. ADDITIONAL INFORMATION

22.1 Professional Confidentiality

As an IT services provider, we may have access to highly confidential and sensitive information about your business operations, systems, and data. We maintain strict professional confidentiality through:

- Non-disclosure agreements with all employees and contractors
- Segregation of client data and systems
- Need-to-know access controls
- Ethical obligations and professional standards

22.2 Subprocessors and Subcontractors

When we engage subcontractors or subprocessors to assist in delivering Services, we ensure they:

- Provide sufficient guarantees of data protection
- Are bound by written contracts with data protection obligations
- Process personal information only on our documented instructions
- Implement appropriate security measures
- Assist us in meeting our data protection obligations

22.3 Industry Standards and Certifications

We strive to maintain industry-recognized security and data protection standards and certifications, which may include:

- ISO 27001 (Information Security Management)
- Cybersecurity frameworks and best practices
- Industry-specific security standards
- Regular third-party security audits

Information about our current certifications is available upon request.

22.4 Data Protection Impact Assessments

For high-risk processing activities, we conduct Data Protection Impact Assessments (DPIAs) to:

- Identify and assess privacy risks
- Determine appropriate mitigation measures
- Ensure compliance with POPIA
- Document our decision-making process

22.5 Records of Processing Activities

We maintain comprehensive records of our processing activities as required by POPIA, including:

- Purposes of processing
- Categories of data subjects and personal information
- Recipients of personal information
- International data transfers
- Retention periods
- Security measures

These records are available to the Information Regulator upon request.

23. INTERPRETATION AND APPLICATION

23.1 Language

This Privacy Policy is available in English. If translated into other languages, the English version shall prevail in the event of any conflict or inconsistency.

23.2 Severability

If any provision of this Privacy Policy is found to be invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect.

23.3 Governing Law

This Privacy Policy is governed by the laws of the Republic of South Africa. Any disputes arising from or related to this Privacy Policy shall be subject to the exclusive jurisdiction of the South African courts.

23.4 Entire Agreement

This Privacy Policy, together with our Website Terms of Use, PAIA Manual, and any applicable service agreements, constitutes the entire agreement between you and Chronologic regarding the processing of your personal information.

23.5 Waiver

Our failure to enforce any provision of this Privacy Policy shall not constitute a waiver of that provision or our right to enforce it in the future.

24. ACKNOWLEDGMENT AND CONSENT

By using our Website or Services, you acknowledge that:

1. You have read and understood this Privacy Policy
2. You understand how we collect, use, and share your personal information
3. You consent to the processing of your personal information as described in this Privacy Policy
4. You understand your rights under POPIA and how to exercise them
5. You know how to contact our Information Officer with questions or complaints
6. You understand your right to withdraw consent or object to processing
7. You are aware of the Information Regulator and how to lodge a complaint

For marketing communications specifically, we will obtain your separate, explicit consent through opt-in mechanisms on our Website or in written communications.

SUMMARY

Your privacy matters to us. This Privacy Policy explains how we collect, use, protect, and share your personal information when you visit our website or use our services. By using our website, you agree to this Privacy Policy.

Key points:

- We collect information to provide and improve our IT services
- We protect your data with industry-leading security measures

- You have rights to access, correct, and delete your information
- We don't sell your personal information to third parties
- You can contact our Information Officer with any privacy concerns

For detailed information, please read the full policy above.

CONCLUSION

Thank you for taking the time to read our Privacy Policy. We are committed to protecting your privacy and handling your personal information responsibly, transparently, and in compliance with all applicable laws.

If you have any questions, concerns, or feedback about this Privacy Policy or our privacy practices, please don't hesitate to contact our Information Officer.

Document Information:

Company: Chronologic Solutions (Pty) Ltd
Registration Number: 2003/003093/07
Effective Date: March 2014
Last Updated: October 2025
Version: 1.11

Information Officer: Natasha Singh
Contact: info@chronologic.co.za | +27 10 591 8105
Website: https://chronologic.co.za

Related Documents:

- PAIA Manual (available at https://chronologic.co.za)
- Website Terms of Use (available at https://chronologic.co.za)
- Cookie Policy (Section 7 of this Privacy Policy)

This Privacy Policy has been prepared in compliance with the Protection of Personal Information Act, 4 of 2013 (POPIA), the Promotion of Access to Information Act, 2 of 2000 (PAIA), and other applicable South African legislation.