Privacy Policy - Bill by asdf consulting (Pty) Ltd

Privacy Policy
1. Introduction
   1.1 About Bill
   1.2 Scope of This Policy
   1.3 Who This Policy Applies To
   1.4 Definition of Personal Information
   1.5 Our Commitment to Privacy
2. Responsible Party and Information Officer
   2.1 Responsible Party
   2.2 Information Officer
3. Personal Information We Collect
   3.1 Information Collected from Law Firms
   3.2 Information Collected from Email Integrations
   3.3 Information Collected from WhatsApp Integration
   3.4 Information Automatically Generated
   3.5 Information from Third-Party Sources
   3.6 Information from Website Analytics
   3.7 Voluntary Provision
4. How We Use Your Personal Information
   4.1 Primary Purposes
   4.2 Lawful Basis for Processing
5. Artificial Intelligence and Automated Processing
   5.1 AI-Powered Matter Detection
   5.2 Transparency About AI Logic
   5.3 AI and WhatsApp Business API Compliance
   5.3A AI Compliance with 2026 WhatsApp Policy
   5.4 Your Rights Regarding AI Processing
6. How We Share Your Personal Information
   6.1 Third-Party Processors (Operators)
   6.2 Data Processing Agreements
   6.3 No Sale of Personal Information
   6.4 Disclosure to Law Firms
   6.5 Legal Disclosures
7. Cross-Border Data Transfers
   7.1 Transfers Outside South Africa
   7.2 Safeguards for Cross-Border Transfers
   7.3 Your Consent to Cross-Border Transfers
8. Data Security and Protection
   8.1 Security Commitment
   8.2 Technical Safeguards
   8.3 Organisational Safeguards

8.4 Multi-Tenancy Data Isolation
8.5 Security Breach Notification
8.6 Limitation of Liability
9. Data Retention and Deletion
9.1 Retention Principle
9.2 Retention Periods
9.3 Legal Retention Requirements
9.4 Deletion After Retention Period
9.5 Exception: Legal Holds
10. Your Rights Under POPIA
10.1 Overview of Rights
10.2 Right to Access (Data Subject Access Request)
10.3 Right to Correction
10.4 Right to Deletion
10.5 Right to Object and Withdraw Consent
10.6 Right to Data Portability
10.7 Right to Lodge a Complaint
10.8 Exercising Your Rights
11. WhatsApp-Specific Privacy Information
11.1 WhatsApp Business API Integration
11.2 WhatsApp Data Handling
11.3 Opt-In for WhatsApp Communications
11.3A Explicit WhatsApp Opt-In (For Clients Receiving Messages)
11.4 Opt-Out of WhatsApp Communications
11.5 WhatsApp Business Policy Compliance
11.6 WhatsApp Privacy Policy
12. Cookies and Website Tracking
12.1 Website Analytics
12.2 Your Rights Regarding Analytics
12.3 No Cookie Consent Banner (Currently)
12.4 No Third-Party Tracking Scripts
12.5 Managing Your Preferences
13. Special Personal Information
13.1 Definition
13.2 Bill's Approach
13.3 Safeguards for Special Personal Information
13.4 Health and Criminal Information
14. Children's Personal Information
14.1 No Intentional Collection
14.2 Inadvertent Collection
14.3 Parental Rights
15. Changes to This Privacy Policy
15.1 Right to Modify
15.2 Notification of Material Changes
15.3 Acceptance of Changes
15.4 Version History
16. International Users and GDPR
16.1 POPIA and GDPR Alignment
16.2 European Users
17. Legal Professional Privilege
17.1 Confidentiality of Legal Communications
17.2 Our Obligations
17.3 No Waiver of Privilege
18. Business Transfers

18.1 Merger, Acquisition, or Sale
19. Contact Us
19.1 Privacy Queries
19.2 Support Queries
20. Complaints and Dispute Resolution
20.1 Internal Complaints
20.2 Information Regulator Complaints
21. Acknowledgements and Consent
21.1 Acknowledgement of Reading
21.2 Specific Consents
21.3 Voluntary Provision
21.4 Right to Withdraw
22. Governing Law
23. Effective Date
Appendix A: Definitions
Appendix B: Summary of Your Rights

Privacy Policy

Effective Date: [Deployment Date - to be set on deployment day] **Last Updated:** 2 January 2026

---

1. Introduction

1.1 About Bill

Bill is an email and WhatsApp billing application developed and operated by **asdf consulting (pty) Ltd.** (registration number: 2023/566704/07) ("**Bill**", "**we**", "**us**", or "**our**"). We are a South African private company with our principal place of business at 2 Blaauwklip Office Park, Webersvallei Road, Stellenbosch, Western Cape, South Africa.

Bill provides automated billing and time tracking services ("**Services**") to South African law firms. Our application automatically tracks email correspondence and WhatsApp messages, detects which legal matters the communications relate to, and creates billable time entries for attorneys.

1.2 Scope of This Policy

This privacy policy explains how we collect, use, store, process, and protect your personal information in accordance with:

- The Protection of Personal Information Act 4 of 2013 ("**POPIA**")
- The Electronic Communications and Transactions Act 25 of 2002 ("**ECT Act**")
- WhatsApp Business API requirements
- All other applicable South African data protection legislation

1.3 Who This Policy Applies To

This privacy policy applies to:

- **Law firms** who subscribe to and use our Services
- **Attorneys** employed by law firms using our Services
- **Clients of law firms** whose information is processed through our Services
- **Any person** whose personal information we collect or process in connection with our Services

1.4 Definition of Personal Information

In this privacy policy, "**Personal Information**" means any information by which you can be identified as an individual or juristic person, including but not limited to:

- Names, email addresses, telephone numbers, postal addresses
- Communication content and metadata
- Client matter information
- Time entry and billing data
- Financial details
- Any other information defined as personal information under POPIA

POPIA uniquely protects both natural persons (individuals) and juristic persons (companies, trusts, partnerships). This privacy policy covers personal information for both.

Examples of juristic person information we process: - Law firm names, registration numbers, and contact details - Client company information (for corporate clients) - Business email addresses and communication metadata - Corporate matter information and billing data

1.5 Our Commitment to Privacy

We recognise the importance of protecting your privacy and the confidential nature of legal communications. We are committed to processing your personal information lawfully, transparently, and securely in accordance with POPIA's eight conditions for lawful processing.

---

2. Responsible Party and Information Officer

2.1 Responsible Party

For purposes of POPIA, we are the "responsible party" in respect of personal information you submit to us through our Services, website (asdf.africa), and any related platforms.

Legal Entity: asdf consulting (pty) Ltd. **Registration Number:** 2023/566704/07 **Physical Address:** 2 Blaauwklip Office Park, Webersvallei Road, Stellenbosch, Western Cape, South Africa **Website:** asdf.africa

2.2 Information Officer

Our designated Information Officer, registered with the Information Regulator, is:

Name: Ricky Klopper **Email:** ricky@asdf.africa **Telephone:** +27 69 0411 717 **Address:** 2 Blaauwklip Office Park, Webersvallei Road, Stellenbosch, Western Cape, South Africa

You may contact our Information Officer regarding any privacy-related queries, data subject access requests, corrections, deletions, objections, or complaints.

---

3. Personal Information We Collect

3.1 Information Collected from Law Firms

When law firms subscribe to our Services, we collect:

- **Firm details:** Firm name, registration number, physical address, contact details
- **Attorney information:** Names, email addresses, telephone numbers, assigned matters, professional details
- **Client information:** Client names, email addresses, contact details, matter descriptions, matter references
- **Account information:** Login credentials, user preferences, subscription details, billing information

3.2 Information Collected from Email Integrations

When attorneys connect their email accounts (Gmail or Microsoft Outlook), we collect:

- **Email metadata:** Sender, recipient, date, time, subject line
- **Email content:** Full message body and content (for matter detection and time entry creation)
- **Attachments:** File names and metadata (content may be processed for billing purposes)
- **Account information:** Email address, account identifiers for OAuth authentication

3.3 Information Collected from WhatsApp Integration

When law firms use our WhatsApp Business API integration, we collect:

- **Message metadata:** Phone numbers, message timestamps, delivery status
- **Message content:** Full WhatsApp message text (for matter detection and time entry creation)
- **WhatsApp profile information:** Business profile name, assigned phone number

3.4 Information Automatically Generated

Our Services automatically generate and store:

- **Time entries:** Billable time descriptions, durations, rates, dates, matter assignments

- **AI analysis results:** Matter detection confidence scores, match types, AI-generated descriptions
- **Usage data:** Login times, features accessed, application activity logs
- **System metadata:** IP addresses, device information, browser type, operating system

3.5 Information from Third-Party Sources

We may collect personal information from:

- **Xero accounting software:** Invoice data, client billing information (if law firm uses Xero integration)
- **Email providers:** Gmail and Microsoft Outlook via OAuth 2.0 authentication
- **WhatsApp Business API:** Via Meta's official Business API platform

3.6 Information from Website Analytics

When you visit our marketing website (asdf.africa), we collect analytics data through Vercel Analytics:

- **Page views and sessions:** Which pages you visit and how long you spend on them
- **Geographic location:** City and country level (derived from IP address)
- **Referral sources:** How you found our website
- **Device and browser information:** Device type, browser type, operating system
- **Anonymised behavioural data:** Navigation patterns and user interactions

Important: Vercel Analytics is privacy-focused and does not use persistent cookies. It uses request-based hashing instead, and session data is automatically discarded after 24 hours. However, under POPIA, you have the right to object to this processing (see Section 10.5).

3.7 Voluntary Provision

The supply of personal information is voluntary; however, certain Services cannot be provided without the necessary information. For example, we cannot create time entries without access to email or WhatsApp communications, and we cannot detect matters without client and matter information.

---

4. How We Use Your Personal Information

4.1 Primary Purposes

We use your personal information for the following purposes:

4.1.1 Billing and Time Tracking

- Create billable time entries from email and WhatsApp communications
- Calculate billable hours and rates
- Generate time entry descriptions
- Associate communications with appropriate matters

4.1.2 Matter Detection

- Use AI-powered analysis (OpenAI GPT-4) to detect which legal matters communications relate to
- Analyse communication content to suggest appropriate matter assignments
- Generate confidence scores for matter matches
- Learn from attorney corrections to improve future detection accuracy

4.1.3 Client and Matter Management

- Maintain client and matter records for law firms
- Track matter assignments and attorney responsibilities
- Organise communications by client and matter

4.1.4 Integration Services

- Connect with email providers (Gmail, Microsoft Outlook) via OAuth 2.0
- Connect with WhatsApp Business API for message processing
- Export time entries to Xero accounting software (if enabled)
- Synchronise data between integrated platforms

4.1.5 Service Provision and Improvement

- Provide access to our platform and Services
- Respond to support queries and technical issues
- Analyse usage patterns to improve features and functionality
- Develop new features and enhancements
- Ensure platform security and prevent fraud

4.1.6 Website Analytics

- Understand how our marketing website is used
- Improve website content and user experience
- Analyse traffic patterns and referral sources
- Optimise website performance

4.1.7 Legal and Regulatory Compliance

- Comply with South African tax, accounting, and legal obligations
- Maintain records as required by the Companies Act, Income Tax Act, and other applicable laws
- Respond to lawful requests from authorities
- Establish, exercise, or defend legal claims

4.2 Lawful Basis for Processing

We process your personal information based on one or more of the following lawful grounds under POPIA:

- **Contractual necessity:** Processing is necessary to perform our Services under our agreement with law firms

- **Consent:** You have provided explicit consent for specific processing activities (particularly for AI processing and cross-border transfers)
- **Legal obligation:** Processing is required to comply with South African tax, accounting, and legal requirements
- **Legitimate interest:** Processing is necessary for our legitimate business interests (service improvement, fraud prevention, website analytics) provided your interests do not override ours

We will make the manner and reason for processing clear to you and will only process personal information where a lawful basis exists. We will not process your personal information for purposes other than those disclosed in this policy without obtaining your explicit consent or demonstrating compatibility with the original purpose.

---

5. Artificial Intelligence and Automated Processing

5.1 AI-Powered Matter Detection

We use artificial intelligence (AI) to assist with matter detection. Specifically, we use OpenAI's GPT-4 language model to analyse the content of emails and WhatsApp messages to determine which legal matters they relate to.

How AI analysis works:

1. Your email or WhatsApp message content is transmitted to OpenAI's API (located in the United States)
2. The AI analyses the communication content alongside your client and matter information
3. The AI suggests which matter the communication relates to and assigns a confidence score
4. The AI generates a suggested time entry description

Important safeguards:

- **Human oversight:** All AI suggestions are reviewed by attorneys before billable time entries are finalised
- **Attorney control:** Attorneys can accept, reject, or modify AI suggestions
- **Not fully automated:** Decisions about billing are not made solely by AI without attorney review
- **Right to object:** You have the right to object to automated processing (see Section 10)

5.2 Transparency About AI Logic

We use the following AI logic to detect matters:

- Pattern matching between communication content and matter descriptions
- Identification of client names, matter references, and legal topics
- Analysis of sender/recipient relationships with known clients
- Contextual understanding of legal terminology and practice areas
- Historical learning from attorney corrections to improve accuracy

If you require more detailed information about our AI logic to enable you to make representations, please contact our Information Officer.

5.3 AI and WhatsApp Business API Compliance

Our use of AI for matter detection is **ancillary to our billing workflow** and complies with WhatsApp Business API requirements. We do not operate a general-purpose AI chatbot. AI is used solely to assist attorneys with billing-related tasks as part of their professional workflow.

5.3A AI Compliance with 2026 WhatsApp Policy

Effective January 15, 2026, Meta updated WhatsApp Business API terms to ban general-purpose AI chatbots from third-party providers. Bill's matter detection feature remains compliant because:

1. **Ancillary Use:** AI is secondary to our primary business function (time entry creation for billing), not the primary service
2. **Structured Process:** Matter detection follows a defined billing workflow, not open-ended conversation
3. **Business-Specific:** AI is used exclusively for legal matter identification within our attorney billing context
4. **Not a Public Assistant:** The AI is internal to the billing platform, not available as a public conversational assistant

This usage aligns with Meta's stated exception: "Structured bots for support, bookings, order tracking, notifications and sales" - our matter detection assists with billing administration.

5.4 Your Rights Regarding AI Processing

Under POPIA Section 71, you have specific rights regarding automated decision-making:

- The right to be informed about AI processing (fulfilled by this policy)
- The right to receive sufficient information about AI logic (available upon request)
- The right to object to automated profiling (see Section 10)
- The right to request human review of AI decisions (attorneys always review AI suggestions)

---

6. How We Share Your Personal Information

6.1 Third-Party Processors (Operators)

We share your personal information with the following third-party service providers who process data on our behalf:

6.1.1 OpenAI (United States)

- **Purpose:** AI-powered matter detection and time entry description generation

- **Data shared:** Email content, WhatsApp message content, client names, matter descriptions
- **Location:** United States
- **Safeguards:** Data processing agreement with POPIA-compliant safeguards, encryption in transit and at rest

6.1.2 Google LLC (International)

- **Purpose:** Gmail integration via OAuth 2.0 for email fetching
- **Data shared:** Email metadata and content, authentication tokens
- **Location:** International infrastructure (including United States, European Union)
- **Safeguards:** OAuth 2.0 authentication, Google's data processing terms, encryption

6.1.3 Microsoft Corporation (International)

- **Purpose:** Outlook integration via OAuth 2.0 for email fetching
- **Data shared:** Email metadata and content, authentication tokens
- **Location:** International infrastructure (including United States, European Union)
- **Safeguards:** OAuth 2.0 authentication, Microsoft's data processing terms, encryption

6.1.4 Meta Platforms, Inc. (International)

- **Purpose:** WhatsApp Business API integration for message processing
- **Data shared:** WhatsApp message content and metadata, business phone numbers
- **Location:** International infrastructure (including United States)
- **Safeguards:** Meta's WhatsApp Business Data Processing Terms, end-to-end encryption (Signal protocol), SOC 2 certification

6.1.5 Xero Limited (United States)

- **Purpose:** Accounting integration for time entry export (if enabled by law firm)
- **Data shared:** Time entries, invoice data, client names, billing amounts
- **Location:** United States (Amazon Web Services data centres). Data is replicated across multiple US locations for availability and disaster recovery. There are no South African-specific data centres.
- **Safeguards:** Standard Contractual Clauses (SCCs) incorporated in Xero's Data Processing Addendum, ISO/IEC 27001:2022 certification, SOC 2 audit reports, industry-standard AES encryption in transit and at rest

6.1.6 Render Services, Inc. (Europe)

- **Purpose:** Cloud hosting infrastructure
- **Data shared:** All data stored in our application database
- **Location:** Frankfurt, Germany (European Union)
- **Safeguards:** ISO 27001 certification, data processing agreement, encryption at rest and in transit

6.1.7 Vercel Inc. (International)

- **Purpose:** Website hosting and analytics for asdf.africa marketing website
- **Data shared:** Website usage data (page views, geographic location, device information)

- **Location:** International infrastructure (United States and global CDN)
- **Safeguards:** Privacy-focused analytics (no persistent cookies), 24-hour data retention, anonymisation by default, no cross-site tracking

6.2 Data Processing Agreements

We have implemented data processing agreements with all third-party processors listed above. These agreements include:

- Obligations to protect personal information with safeguards substantially similar to POPIA's conditions
- **Provisions covering juristic person protection (unique to POPIA):** All processors acknowledge that POPIA protects both natural persons (individuals) and juristic persons (companies, trusts, partnerships), and agree to apply equivalent safeguards to business-related personal information including company names, registration numbers, and business contact details
- Restrictions on further processing and sub-processing
- Security and confidentiality obligations
- Data breach notification requirements
- Rights to audit compliance

6.3 No Sale of Personal Information

We do not sell, rent, or trade your personal information to third parties for marketing or any other purposes.

6.4 Disclosure to Law Firms

Personal information about communications is accessible to:

- The law firm that subscribes to our Services
- Attorneys within that firm who are assigned to relevant matters
- Law firm administrators with appropriate access permissions

We implement strict **multi-tenancy data isolation** to ensure that law firms can only access their own data and cannot access data belonging to other law firms.

6.5 Legal Disclosures

We may disclose personal information if required to do so by law, court order, or governmental authority, including but not limited to:

- Compliance with subpoenas or court orders
- Cooperation with law enforcement investigations
- Protection of our legal rights or the rights of others
- Prevention of fraud or security threats

---

7. Cross-Border Data Transfers

7.1 Transfers Outside South Africa

Your personal information may be transferred to and processed in countries outside South Africa, including the United States and the European Union.

Specifically, personal information is transferred to:

- **United States:** OpenAI (AI processing), Google (Gmail API), Microsoft (Outlook API), Meta (WhatsApp Business API), Xero (accounting integration via AWS), Vercel (website analytics)
- **European Union:** Render Services (cloud hosting in Frankfurt, Germany)
- **Other jurisdictions:** Potentially other countries where our third-party processors maintain infrastructure

7.2 Safeguards for Cross-Border Transfers

We ensure adequate protection for cross-border transfers through:

7.2.1 Data Processing Agreements

All international processors are bound by data processing agreements containing safeguards substantially similar to POPIA's eight conditions, including provisions protecting juristic persons.

7.2.2 Contractual Necessity

Transfers are necessary for the performance of our Services under our contract with law firms. Without these transfers, we cannot provide AI-powered matter detection, email integration, or cloud hosting.

7.2.3 Adequate Protection Standards

Our third-party processors maintain: - Industry-standard security certifications (ISO 27001, SOC 2) - Encryption in transit (TLS/HTTPS) and at rest - Access controls and authentication measures - Incident response and breach notification procedures - GDPR compliance (where applicable, providing similar protections to POPIA)

7.3 Your Consent to Cross-Border Transfers

By using our Services, you consent to the cross-border transfer of your personal information to the countries and processors listed above for the purposes described in this privacy policy.

If you do not consent to cross-border transfers, you may not be able to use our Services, as these transfers are essential to our platform's functionality.

---

8. Data Security and Protection

8.1 Security Commitment

As a platform processing confidential legal communications, we recognise that protecting your personal information is of paramount importance. We implement appropriate technical and organisational safeguards to protect personal information against loss, damage, unauthorised access, alteration, disclosure, or destruction.

8.2 Technical Safeguards

Encryption: - All data transmitted between your devices and our servers is encrypted using TLS (Transport Layer Security) - Data stored in our database is encrypted at rest - Email and WhatsApp communications are encrypted during transmission to third-party APIs

Authentication and Access Control: - OAuth 2.0 authentication for email integrations (no password storage) - Secure session management with token-based authentication - Role-based access controls within law firms - Multi-tenancy architecture preventing cross-firm data access

Infrastructure Security: - Cloud hosting with ISO 27001 certified provider (Render Services) - Regular security updates and patching - Firewall protection and intrusion detection - Secure database configuration with restricted access

8.3 Organisational Safeguards

Access Restrictions: - Personal information accessible only to employees and contractors who require access to perform their duties - All personnel with access are bound by confidentiality obligations - Principle of least privilege applied to system access

Policies and Procedures: - Data protection policies and procedures documented and enforced - Regular security training for staff - Incident response plan for security breaches - Continuous monitoring and improvement of security measures

8.4 Multi-Tenancy Data Isolation

Firm boundary enforcement is critical to our security architecture. Every database query is filtered by law firm to ensure:

- Law firms can only access their own data
- Attorneys can only view matters assigned to their firm
- Clients of one firm cannot see data belonging to other firms
- Cross-firm data leakage is prevented at the database level

We conduct regular security audits to verify the integrity of our multi-tenancy isolation.

8.5 Security Breach Notification

In accordance with POPIA Section 22 and the 2025 amendments, if we become aware of a security compromise (data breach) that affects your personal information, we will:

1. **Assess the breach:** Determine the scope, nature, and impact
2. **Notify the Information Regulator:** Report the breach via the eServices Portal (https://eservices.inforegulator.org.za) as soon as reasonably possible after discovery, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and restore system integrity
3. **Notify affected data subjects:** Where required by law, inform you of the breach, its likely consequences, and measures taken
4. **Document the breach:** Maintain records of the incident and our response for a minimum of two years, which may be subject to review by the Information Regulator

8.6 Limitation of Liability

Despite our security measures, **no internet transmission or electronic storage system is completely secure**. We cannot guarantee absolute security of your personal information. By using our Services, you acknowledge that you transmit personal information at your own risk. Once we receive your information, we will use the safeguards described above to protect it.

---

9. Data Retention and Deletion

9.1 Retention Principle

We retain personal information only as long as necessary for the purposes described in this privacy policy or as required by South African law.

9.2 Retention Periods

We apply the following retention periods:

Data Type	Retention Period	Legal Basis
Time entries and invoices	7 years from date of invoice	Companies Act, Section 24 (company records must be kept for 7 years)
Client and matter records	7 years from last activity	Companies Act (longest applicable retention period)
Email communications	7 years from associated invoice date	Aligned with billing records for audit and dispute purposes
WhatsApp communications	7 years from associated invoice date	Aligned with billing records for audit and dispute purposes

Data Type	Retention Period	Legal Basis
User accounts	Duration of active subscription + 30 days	Contractual necessity
Usage logs	12 months	Legitimate interest (security and service improvement)
Website analytics data	24 hours	Automatic deletion by Vercel Analytics

9.3 Legal Retention Requirements

Our retention periods are based on the following South African legal requirements:

- **Companies Act, Section 24:** Company documents, accounts, books, and records must be retained for 7 years
- **Income Tax Act:** Tax records and invoices must be retained for 5 years
- **FICA (Financial Intelligence Centre Act):** Client identification records must be retained for 5 years
- **Legal Practice Council Rule 54.9.2:** Law firms must retain accounting records and all files and documents relating to matters dealt with on behalf of clients for at least seven years from the date of the last entry

Where multiple retention periods apply, we apply the longest period to ensure comprehensive compliance.

9.4 Deletion After Retention Period

Once retention periods expire, we will delete personal information as soon as reasonably practicable using secure deletion methods that prevent reconstruction of the information in intelligible form.

Deletion methods: - Secure database deletion with overwriting - Encryption key destruction (for encrypted backups) - Removal from all active systems and backups

Deletion logs: We maintain audit logs of deletion activities to demonstrate compliance with retention obligations.

9.5 Exception: Legal Holds

We may retain personal information beyond the stated retention periods if:

- Required by court order or legal process
- Necessary for ongoing litigation or dispute
- Required by a regulatory authority
- Needed to establish, exercise, or defend legal claims

In such cases, we will document the justification for extended retention and delete the information once the legal hold is lifted.

---

10. Your Rights Under POPIA

10.1 Overview of Rights

Under POPIA, you have the following rights regarding your personal information:

1. **Right to access** your personal information
2. **Right to correct** inaccurate or incomplete information
3. **Right to deletion** when no longer needed (subject to legal retention requirements)
4. **Right to object** to processing on legitimate grounds
5. **Right to data portability** (export your data in a structured format)
6. **Right to withdraw consent** where processing is based on consent
7. **Right to lodge a complaint** with the Information Regulator

These rights apply to both natural persons (individuals) and juristic persons (companies, trusts). If you are a company, trust, or other legal entity, you may exercise these rights in respect of your organisation's personal information.

10.2 Right to Access (Data Subject Access Request)

You have the right to request access to your personal information.

How to request access: - Email our Information Officer at ricky@asdf.africa - Send an SMS or WhatsApp message to +27 69 0411 717 - Submit a written request by post to our physical address - Request access via any other reasonable channel

What we will provide: - Copies of all personal information we hold about you - Information about how we use your personal information - Information about third parties with whom we have shared your information - Export in a structured, commonly used format (CSV or JSON)

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

Cost: Access requests are **free of charge**.

10.3 Right to Correction

You have the right to request correction of inaccurate or incomplete personal information.

How to request correction: - Email ricky@asdf.africa with details of the correction needed - SMS or WhatsApp +27 69 0411 717 with correction request - Submit a written request by post - Use any other expedient channel (hand delivery, fax, etc.)

What we will do: - Assess the accuracy of the information - Make corrections within 30 days where information is inaccurate or incomplete - Notify you of the action taken - Update records and notify third parties if information was shared

Response timeframe: 30 days from receipt of request.

10.4 Right to Deletion

You have the right to request deletion of your personal information when it is no longer needed for the original purpose.

How to request deletion: - Email ricky@asdf.africa with deletion request - SMS or WhatsApp +27 69 0411 717 with deletion request - Submit a written request via any accessible channel

Important limitations: - We may refuse deletion if retention is required by South African law (see Section 9.2) - We may refuse deletion if needed for establishment, exercise, or defence of legal claims - We may refuse deletion if required for compliance with legal obligations

What we will do: - Assess whether deletion is permissible under POPIA and other applicable laws - Securely delete information preventing reconstruction (where permissible) - Respond within 30 days explaining action taken or justification for refusal

Response timeframe: 30 days from receipt of request.

10.5 Right to Object and Withdraw Consent

You have the right to object to processing on legitimate grounds or withdraw consent at any time.

How to object or withdraw consent: - Email ricky@asdf.africa - SMS or WhatsApp +27 69 0411 717 - Submit objection via any expedient, accessible channel - **Free of charge** (2025 POPIA amendment)

Effect of withdrawal: - We will cease processing for objected purposes unless we have overriding legitimate grounds - Withdrawal does not affect the lawfulness of processing prior to withdrawal - We may be unable to provide certain Services if consent is withdrawn (e.g., AI processing, cross-border transfers)

Specific objections: - **AI processing:** You can object to automated matter detection (we will revert to manual matter assignment) - **Cross-border transfers:** You can object to transfers (we may be unable to provide Services) - **Website analytics:** You can object to Vercel Analytics tracking (contact us to opt out) - **Marketing communications:** You can opt out at any time (though Bill does not currently send marketing)

Response timeframe: We will process objections and consent withdrawals within 24 hours where technically feasible.

10.6 Right to Data Portability

You have the right to receive your personal information in a structured, commonly used, machine-readable format.

How to request data portability: - Email ricky@asdf.africa with export request

What we will provide: - Time entries (CSV or JSON format) - Email metadata (CSV or JSON format) - WhatsApp message metadata (CSV or JSON format) - Client and matter records (CSV or JSON format) - Invoice data (CSV or JSON format)

Response timeframe: 30 days from receipt of request.

10.7 Right to Lodge a Complaint

You have the right to lodge a complaint with the Information Regulator if you believe we have violated your privacy rights.

Information Regulator South Africa:

General Enquiries: - Toll-Free: 0800 017 160 - Landline: 010 023 5200 - Email: enquiries@inforegulator.org.za

POPIA Complaints: - Email: POPIAComplaints@inforegulator.org.za

Physical Address: Woodmead North Office Park 54 Maxwell Drive Woodmead, Johannesburg, 2191 South Africa

Website: https://inforegulator.org.za

eServices Portal: https://eservices.inforegulator.org.za

We encourage you to contact us first so we may attempt to resolve your concern. However, you have the right to lodge a complaint with the Information Regulator at any time.

10.8 Exercising Your Rights

Multi-channel access (2025 POPIA amendment): You may exercise your rights via: - Email: ricky@asdf.africa - SMS: +27 69 0411 717 - WhatsApp: +27 69 0411 717 - Post: 2 Blaauwklip Office Park, Webersvallei Road, Stellenbosch, Western Cape - Hand delivery: Same address - Fax: N/A - Any other manner that is expedient, reasonably accessible, and free of charge to you

No charge: Exercising your rights is free of charge.

Verification: We may verify your identity before fulfilling requests to protect against unauthorised access to personal information.

---

11. WhatsApp-Specific Privacy Information

11.1 WhatsApp Business API Integration

Bill uses the official WhatsApp Business API to enable law firms to create billable time entries from WhatsApp messages sent to designated business phone numbers.

11.2 WhatsApp Data Handling

Message storage: - WhatsApp messages are encrypted end-to-end using the Signal protocol during transmission - Once delivered to our platform, messages are stored in our database (encrypted at rest) - We retain WhatsApp messages for 7 years aligned with

billing records (see Section 9.2) - WhatsApp Cloud API stores messages for a maximum of 30 days, then deletes them

What we collect from WhatsApp: - Message content (text messages sent to your law firm's WhatsApp Business number) - Message metadata (timestamp, sender phone number, delivery status) - Business profile information (your firm's WhatsApp Business profile name)

11.3 Opt-In for WhatsApp Communications

By sending a WhatsApp message to your law firm's designated Bill phone number, you are opting in to receive responses via WhatsApp.

What you can expect: - Confirmation messages acknowledging receipt of your time entry - Notifications about time entry creation or errors - Responses to queries about your message

Types of messages (Meta categories): - **Utility messages:** Confirmations, notifications about time entry status - **Authentication messages:** Verification codes (if implemented) - We do **not** send marketing messages via WhatsApp

11.3A Explicit WhatsApp Opt-In (For Clients Receiving Messages)

If your law firm sends proactive WhatsApp notifications to clients (beyond immediate responses), explicit consent is required before the first message is sent. The opt-in must include:

1. **Clear Statement:** "I consent to receive WhatsApp messages from [Law Firm Name] about my legal matters"
2. **Business Name:** [Law Firm Name] (if Bill sends on behalf of firm)
3. **Message Types:** Clients can expect to receive:
    - Utility messages: Case updates, document requests, appointment confirmations
    - Authentication messages: Verification codes (if implemented)
    - We do **not** send promotional or marketing messages

Law Firm Responsibility: Law firms using Bill are responsible for obtaining this explicit consent from their clients BEFORE sending any proactive WhatsApp messages. Bill does not initiate contact with customers or send unsolicited messages.

Bill's Role: Bill's platform enables attorneys to create time entries from WhatsApp messages that clients send to the law firm's designated business number. We do not market to or contact clients on behalf of law firms.

11.4 Opt-Out of WhatsApp Communications

You can opt out of WhatsApp communications at any time.

How to opt out: - Reply "STOP" to any WhatsApp message from Bill - Email ricky@asdf.africa requesting opt-out - Contact your law firm to request removal from WhatsApp billing

Processing time: We will process opt-out requests within 24 hours and cease sending WhatsApp messages to your number.

11.5 WhatsApp Business Policy Compliance

Bill complies with WhatsApp's Business Policy, including: - No use of WhatsApp data for purposes other than messaging - No sharing of sensitive identifiers (payment card numbers, financial account numbers, ID numbers) - No general-purpose AI chatbots (our AI is ancillary to billing workflow, not conversational) - Respect for opt-out requests within 24 hours

11.6 WhatsApp Privacy Policy

WhatsApp's own privacy practices are governed by Meta's privacy policies: - WhatsApp Privacy Policy - WhatsApp Business Privacy Policy

We recommend reviewing WhatsApp's privacy policies to understand how Meta processes WhatsApp communications.

---

12. Cookies and Website Tracking

12.1 Website Analytics

Our marketing website (asdf.africa) uses Vercel Analytics to understand how the website is used and to improve user experience.

What Vercel Analytics collects: - Page views and user sessions - Geographic location (city and country level from IP address) - Referral sources (how you found our website) - Device and browser information - Anonymised behavioural data (navigation patterns)

Privacy-focused approach: - **No persistent cookies:** Vercel Analytics does not use traditional cookies - **No cross-site tracking:** Your activity is not tracked across other websites - **No third-party data sharing:** Analytics data is not shared with third parties - **24-hour data retention:** Session data is automatically discarded after 24 hours - **Request-based hashing:** User identification uses temporary request hashing instead of persistent identifiers

12.2 Your Rights Regarding Analytics

Even though Vercel Analytics is privacy-focused and cookie-free, under POPIA you have the right to:

- **Object to analytics tracking:** Contact ricky@asdf.africa to opt out of website analytics
- **Request your data:** Request what analytics data we have collected about your website visits
- **Request deletion:** Request deletion of any analytics data associated with you

12.3 No Cookie Consent Banner (Currently)

Important notice: Our website currently does not have a cookie consent banner or opt-in mechanism. While Vercel Analytics is privacy-friendly and does not use persistent cookies, we recognise that under POPIA, even privacy-focused analytics may require user consent.

We are working to implement: - A cookie consent banner that allows you to opt out of analytics before any tracking occurs - Conditional loading of Vercel Analytics based on your consent - A cookie preference centre for managing your choices

Until this implementation is complete, analytics tracking occurs automatically when you visit our website. If you object to this, please contact ricky@asdf.africa.

12.4 No Third-Party Tracking Scripts

We do **not** use any third-party tracking technologies on our website, including: - Google Analytics - Meta Pixel / Facebook Pixel - Hotjar, Amplitude, Mixpanel, or similar tracking tools - Advertising cookies or retargeting pixels

The only analytics implementation is Vercel Analytics as described above.

12.5 Managing Your Preferences

You can control website tracking through: - Contacting ricky@asdf.africa to opt out of analytics (we will manually exclude your IP address) - Your browser settings (block scripts or use privacy mode) - Browser extensions that block analytics scripts

Declining analytics tracking will not affect your ability to use our website or Services.

---

13. Special Personal Information

13.1 Definition

"**Special Personal Information**" under POPIA means personal information concerning:

- Religious or philosophical beliefs
- Race or ethnic origin
- Trade union membership
- Political opinions
- Health or sex life
- Biometric information
- Criminal behaviour or criminal history

13.2 Bill's Approach

We generally do not intentionally collect Special Personal Information. However, legal communications may occasionally reference health-related legal matters (e.g., medical malpractice cases) or criminal defence cases.

13.3 Safeguards for Special Personal Information

If Special Personal Information is inadvertently processed:

- We process only where necessary for legal claims or contractual performance
- We apply heightened security safeguards
- We limit access to authorised personnel
- We do not use Special Personal Information for profiling or marketing

13.4 Health and Criminal Information

If you are concerned about Special Personal Information in your communications:

- Contact our Information Officer to discuss specific safeguards
- Request redaction of sensitive information (where legally permissible)
- Exercise your right to object to processing (see Section 10.5)

---

14. Children's Personal Information

14.1 No Intentional Collection

Bill does not intentionally collect personal information about children (individuals under 18 years of age). Our Services are designed for use by law firms and attorneys, not children.

14.2 Inadvertent Collection

If personal information about a child is inadvertently collected through legal communications (e.g., family law matters involving children):

- We process only with consent of a competent person (parent/guardian) or where necessary for legal claims
- We apply heightened protection safeguards
- We comply with POPIA's special requirements for children's data

14.3 Parental Rights

If you are a parent or guardian and believe we have collected personal information about your child, please contact our Information Officer at ricky@asdf.africa to exercise rights on the child's behalf.

---

15. Changes to This Privacy Policy

15.1 Right to Modify

We reserve the right to update this privacy policy from time to time to reflect:

- Changes in our Services or features
- Changes in applicable laws or regulations
- New third-party processors or integrations
- Improved privacy practices

15.2 Notification of Material Changes

We will notify you of material changes to this privacy policy by:

- Email to your registered email address (for law firm administrators)
- Prominent notice on our website and platform
- At least 30 days' advance notice before changes take effect

15.3 Acceptance of Changes

Your continued use of our Services after changes take effect indicates acceptance of the updated privacy policy.

If you do not agree to the changes, you may: - Contact us to discuss your concerns - Withdraw consent and cease using our Services - Exercise your right to deletion (subject to legal retention requirements)

15.4 Version History

Significant versions of this privacy policy are archived and available upon request from our Information Officer.

---

16. International Users and GDPR

16.1 POPIA and GDPR Alignment

While Bill is a South African company operating under POPIA, we recognise that POPIA is substantially aligned with the European Union's General Data Protection Regulation (GDPR). Many of the rights and safeguards described in this privacy policy are similar to GDPR requirements.

16.2 European Users

If you are located in the European Economic Area (EEA), you may have additional rights under GDPR, including:

- Right to restriction of processing
- Right to object to legitimate interest processing
- Right to lodge a complaint with your local data protection authority

Please contact our Information Officer if you wish to exercise GDPR-specific rights.

---

17. Legal Professional Privilege

17.1 Confidentiality of Legal Communications

We recognise that communications processed through Bill may be subject to legal professional privilege and attorney-client confidentiality.

17.2 Our Obligations

We treat all communications processed through our platform as:

- Strictly confidential (whether legally privileged or not)
- Subject to heightened security safeguards
- Accessible only to authorised personnel within the relevant law firm

17.3 No Waiver of Privilege

Use of our Services does not constitute a waiver of legal professional privilege. We implement measures to preserve the privileged status of communications.

---

18. Business Transfers

18.1 Merger, Acquisition, or Sale

In the event that asdf consulting (pty) Ltd. is involved in a merger, acquisition, sale of assets, or bankruptcy:

- Your personal information may be transferred to a successor entity
- We will provide notice before personal information is transferred and becomes subject to a different privacy policy
- The successor entity will be bound to protect your personal information in accordance with this privacy policy until you are notified of changes

---

19. Contact Us

19.1 Privacy Queries

For questions about this privacy policy, our data practices, or to exercise your rights:

Information Officer: Ricky Klopper **Email:** ricky@asdf.africa **Telephone:** +27 69 0411 717 **SMS/WhatsApp:** +27 69 0411 717 **Physical Address:** 2 Blaauwklip Office Park, Webersvallei Road, Stellenbosch, Western Cape, South Africa

19.2 Support Queries

For technical support or account-related queries (not privacy-related):

Email: support@asdf.africa **Website:** asdf.africa

---

20. Complaints and Dispute Resolution

20.1 Internal Complaints

If you believe we have violated your privacy rights, we encourage you to contact us first:

Email: ricky@asdf.africa **Subject Line:** “Privacy Complaint”

We will: - Acknowledge your complaint within 3 business days - Investigate your complaint thoroughly - Respond with our findings and proposed resolution within 30 days

20.2 Information Regulator Complaints

You have the right to lodge a complaint with the Information Regulator at any time, whether or not you have contacted us first:

Information Regulator South Africa

POPIA Complaints: Email: POPIAComplaints@inforegulator.org.za

General Enquiries: Toll-Free: 0800 017 160 Landline: 010 023 5200 Email: enquiries@inforegulator.org.za

Physical Address: Woodmead North Office Park 54 Maxwell Drive Woodmead, Johannesburg, 2191 South Africa

Website: https://inforegulator.org.za **eServices Portal:** https://eservices.inforegulator.org.za

---

21. Acknowledgements and Consent

21.1 Acknowledgement of Reading

By using our Services, you acknowledge that you have read, understood, and agree to be bound by this privacy policy.

21.2 Specific Consents

By using our Services, you specifically consent to:

1. **AI Processing:** Use of OpenAI's artificial intelligence to analyse your communications for matter detection
2. **Cross-Border Transfers:** Transfer of your personal information to the United States, European Union, and other jurisdictions as described in Section 7
3. **Third-Party Processing:** Sharing of your personal information with the third-party processors listed in Section 6
4. **WhatsApp Processing:** Collection and processing of WhatsApp messages sent to your law firm's Bill number
5. **7-Year Retention:** Retention of billing-related communications for 7 years as required by South African law
6. **Website Analytics:** Collection of anonymised website usage data through Vercel Analytics

21.3 Voluntary Provision

You acknowledge that providing personal information is voluntary, but certain Services cannot be provided without the necessary information.

21.4 Right to Withdraw

You may withdraw any consent at any time (see Section 10.5), though this may affect our ability to provide Services.

---

22. Governing Law

This privacy policy is governed by and interpreted in accordance with the laws of the Republic of South Africa, including POPIA, the Electronic Communications and Transactions Act, and all other applicable data protection legislation.

---

23. Effective Date

This privacy policy is effective as of the date it is deployed and published to asdf.africa/privacy-policy.

The effective date will be set when this policy is deployed and made accessible to the public. Until deployment, this policy is in draft form.

Under POPIA, privacy policies for new services may be effective immediately upon deployment. There is no mandatory advance notice period for initial privacy policies. This policy will take effect on the day it is published and made available at all points of information collection.

Deployment Checklist (Internal Reference): - [ ] Website asdf.africa confirmed live and accessible - [ ] Privacy policy published at https://asdf.africa/privacy-policy - [ ] URL tested for accessibility from external networks - [ ] Deployment date recorded in version control - [ ] Privacy policy URL added to Meta app settings - [ ] Effective date updated to deployment date

Last Updated: 2 January 2026

Appendix A: Definitions

AI (Artificial Intelligence): Machine learning technology used to analyse communications and detect legal matters.

Data Subject: Any person (natural or juristic) whose personal information is processed by Bill.

Information Officer: Person designated under POPIA to oversee data protection compliance (registered with Information Regulator).

Juristic Person: A legal entity such as a company, trust, partnership, or other organisation (POPIA protects both natural and juristic persons).

Operator: Third-party processor who processes personal information on behalf of Bill (e.g., OpenAI, Google, Microsoft).

Personal Information: Information by which a natural or juristic person can be identified, as defined by POPIA.

POPIA: Protection of Personal Information Act 4 of 2013 (South African data protection law).

Responsible Party: asdf consulting (pty) Ltd., the entity that determines the purpose and means of processing personal information.

Special Personal Information: Sensitive categories of personal information (health, race, religion, criminal history, etc.) with heightened protection under POPIA.

Appendix B: Summary of Your Rights

Right	Description	How to Exercise	Response Time
Access	Request copies of your personal information	Email ricky@asdf.africa	30 days
Correction	Request correction of inaccurate information	Email, SMS, WhatsApp ricky@asdf.africa	30 days
Deletion	Request deletion (subject to legal retention)	Email, SMS, WhatsApp ricky@asdf.africa	30 days

Right	Description	How to Exercise	Response Time
Objection	Object to processing or withdraw consent	Email, SMS, WhatsApp ricky@asdf.africa	24 hours
Portability	Receive data in machine-readable format	Email ricky@asdf.africa	30 days
Complaint	Lodge complaint with Information Regulator	POPIAComplaints@inforegulator.org.za	Per Regulator

All rights are free of charge and accessible via multiple channels (email, SMS, WhatsApp, post, hand delivery).

END OF PRIVACY POLICY

---

asdf consulting (pty) Ltd. Registration Number: 2023/566704/07 2 Blaauwklip Office Park, Webersvallei Road, Stellenbosch, Western Cape, South Africa Website: asdf.africa Email: ricky@asdf.africa