

Privacy Policy

Version 1.0 | Effective: August 2026 | Last Updated: August 2026

Privacy inquiries: hello@dahnjay.tech | dahnjay.tech

& ATTORNEY REVIEW PENDING — DRAFT

This is an operational/legal draft. It has not been finalized by legal counsel. Sections involving jurisdiction-specific rights, international transfers, data retention periods, and legal bases for processing require attorney review before final publication. Internal status: Attorney Review Pending.

TABLE OF CONTENTS

1. About This Policy & Who We Are
2. Scope
3. Information We Collect
4. Information You Provide to Us
5. Information Collected Automatically
6. Information from Connected Services & Integrations
7. Artificial Intelligence Privacy
8. Business Memory & Customer-Owned Data
9. Employee & Workforce Information
10. Location Data (GPS Clock-In)
11. Communications Privacy (Phone, SMS, WhatsApp, Email)
12. Payment & Billing Information
13. Support & Refund Evidence
14. How We Use Your Information
15. How We Share Information
16. Third-Party Service Providers & Subprocessors
17. Selling Data
18. Children & Minors
19. International Data Processing
20. Data Retention
21. Your Privacy Rights
22. How to Submit a Privacy Request
23. Security
24. Security Incidents
25. Cookies & Browser Storage
26. Policy Changes
27. Contact

1. About This Policy & Who We Are

Dahn Jay Tech ("DJT," "we," "our," or "us") operates an AI-powered business platform serving businesses in the United States, Kenya, and other markets. This Privacy Policy explains how DJT collects, uses, shares, stores, and protects information in connection with DJT services.

We are committed to being transparent about what we do with information. This policy is written for business customers — the organizations that use DJT — as well as for individuals whose information may be processed through DJT's platform.

Privacy inquiries and requests may be submitted to: hello@dahnjay.tech

2. Scope

This Privacy Policy applies to all DJT services, including the DJT web platform, Atlas AI, Business Memory, Pulse, workforce and payroll tools, communications features (email, phone, SMS, WhatsApp), educational courses, mobile PWA access, and all associated APIs and integrations.

This policy does not govern the separate privacy practices of third-party services that DJT integrates with (such as Google, Microsoft, Telnyx, Stripe, Flutterwave, WhatsApp/Meta, or OpenAI). Those services have their own privacy policies.

DJT serves both the United States and Kenya. Certain rights described in this policy may vary depending on your jurisdiction and applicable law.

3. Information We Collect

DJT processes information across several categories based on how you use the platform. The table below summarizes the main types:

Account Information	Name, email address, phone number, authentication credentials, organization affiliation, account role, login and session records.
Business Information	Legal business name, trade name, business address, country, industry, EIN (US) or KRA PIN (Kenya), business hours, subdomain, tenant configuration, business verification records.
Employee & Workforce	Employee names, contact information, employee ID, job title, department, schedule, payroll-related data, attendance records, clock-in/out timestamps, employment status, onboarding information.
Location Information	GPS coordinates and timestamps collected at the moment of authorized clock-in/out events. DJT collects location only during specific platform actions — not continuously in the background.
Business Memory & Knowledge	Business instructions, policies, FAQs, operating procedures, uploaded documents (menus, brochures, price lists, policies), and context provided to Atlas and other AI tools.
AI Interaction Records	Prompts and questions submitted to Atlas, AI-generated responses, conversation context, session metadata, usage records, and AI provider request metadata.
Communications Records	Email metadata and content where authorized, SMS content, WhatsApp messages, phone call metadata, call recordings (where enabled), AI-generated call transcripts and summaries, appointment requests, and lead inquiries.
Payment & Subscription	Subscription plan, billing cycle, transaction history, invoice records, DJT Credit balances and ledger, payment provider IDs, payment status, and refund/dispute records.
Integration Information	OAuth connection status, third-party account IDs, integration configuration, webhook event logs, and encrypted credential tokens where applicable.
Security & Technical	IP address, device type, browser, session metadata, login history, security events, audit logs, API request metadata, timestamps, error information, and suspicious activity records.
Support Information	Support ticket content, screenshots and uploaded files submitted during support, correspondence, diagnostic references, refund and dispute evidence, and privacy request records.
Course Records	Course purchases, progress records, lesson completion data, and implementation support case records.

4. Information You Provide to Us

DJT receives information directly when you:

- Create a DJT account and complete business onboarding.
- Configure your business profile, Business Memory, product catalogue, FAQs, or Atlas settings.
- Add employees, configure schedules, or enter payroll-related information.
- Connect integrations (Google, Microsoft 365, Telnyx, Stripe, Flutterwave, WhatsApp, and others).
- Upload documents, images, or files.
- Contact DJT support, submit tickets, or upload evidence.
- Provide AI prompts or interact with Atlas and other AI employees.
- Purchase subscriptions, Credits, or courses.
- Complete onboarding attestations (Terms acceptance, prohibited-business declaration, minor-data declaration).

5. Information Collected Automatically

DJT and its infrastructure providers automatically collect certain technical information when you use the platform, including:

- Login and session activity — timestamps, IP addresses, authentication events.
- Security events — failed login attempts, MFA events, suspicious activity.
- Usage data — features accessed, pages visited, actions taken within DJT.
- Device and browser information — browser type and version, operating system.
- API request metadata — request timestamps, response status, performance data.
- Error logs — error types, affected components, timestamps.
- Cookies and local storage — DJT uses essential authentication cookies and browser storage to maintain your session and platform state. See Section 25 for details.

6. Information from Connected Services & Integrations

When you connect third-party accounts to DJT, we receive only the information within the scopes you authorize:

- Google / Gmail: Email metadata and content within authorized scopes, calendar data where connected, authentication identity.
- Microsoft 365 / Outlook: Email metadata and content within authorized scopes, calendar data where connected, organizational identity.
- Telnyx: Call metadata, telephony event data, phone number configuration, SMS delivery records.
- Stripe: Subscription status, payment events, invoice identifiers, dispute notifications. Full card numbers are handled by Stripe, not stored by DJT.
- Flutterwave: Payment events, transaction status, relevant identifiers. Complete payment card data is handled by Flutterwave, not stored by DJT.
- M-Pesa infrastructure: Payment confirmation and status records.
- Wise: Transfer confirmation and status records where applicable.
- WhatsApp / Meta: Messaging events within the WhatsApp Business API, message delivery status.

DJT receives only what the connected service provides within the permissions you grant. You can disconnect integrations at any time from your DJT account settings. Disconnecting an integration may affect related features.

7. Artificial Intelligence Privacy

DJT's AI systems — including Atlas and other AI workforce agents — process information to deliver AI-powered features. Here is what you should know:

What AI Processes

- Prompts and questions you or your customers submit to AI-powered features.
- Business Memory and Knowledge Base content you have configured.
- Conversation history within the applicable session or memory context.
- Uploaded documents and structured information provided to Atlas.

Infrastructure Providers

DJT processes AI requests through authorized model and infrastructure providers (which may include services such as Anthropic and OpenAI). Customer information submitted to AI features may be transmitted to these providers to generate responses. These providers operate under their own data processing terms. DJT selects providers based on service quality and data protection considerations.

DJT does not represent that AI providers never receive or process any customer data — AI providers receive request data necessary to generate responses. DJT does not represent that providers never retain any data without verifying the current contractual and technical status. If you have specific questions about AI provider data handling, contact hello@dahnjay.tech.

Tenant Isolation

DJT's architecture is designed so that one customer's private Business Memory is not intentionally made available to another customer's AI experience. Each business tenant's data is logically separated. DJT applies Row-Level Security and tenant-scoped access controls across its database and AI retrieval systems to enforce this isolation.

AI Output Accuracy

AI-generated outputs may contain errors, incomplete information, or outdated content. DJT does not guarantee AI accuracy. Customers remain responsible for reviewing AI output before relying on it for important business, legal, financial, employment, or medical decisions.

8. Business Memory & Customer-Owned Data

Customers retain ownership of the business content they submit to DJT, including Business Memory, uploaded documents, configurations, employee information, and other customer-originated data.

DJT receives the limited license necessary to store, process, transmit, analyze, generate outputs from, and back up that content for the purpose of delivering DJT's services. DJT does not claim ownership of customer business content and does not use customer Business Memory for purposes outside service delivery without your authorization.

DJT does not sell customer business content. Customer content is processed to operate DJT, respond to your Atlas requests, and provide other platform features you have activated.

9. Employee & Workforce Information

DJT customers who use workforce, payroll, attendance, and HR tools may process information relating to their employees or workers through DJT.

Important: The employer (DJT customer) is responsible for deciding what workforce information to enter into DJT, ensuring employees are informed as required by applicable law, obtaining necessary consents or authorizations, and complying with applicable employment privacy laws. DJT processes workforce information to provide services requested by the employer.

DJT processes employee information to support timekeeping, payroll workflows, scheduling, onboarding, and workforce management. Employees whose information is processed through DJT may be subject to their employer's privacy policies in addition to DJT's.

DJT is not the employer of any employee whose information is processed through the platform. Responsibility for workforce data decisions, employment notices, and payroll accuracy rests with the DJT customer.

10. Location Data — GPS Clock-In

DJT's clock-in feature uses GPS location data to support attendance verification for authorized workforce management purposes.

- **When collected:** Location is captured at the moment an employee performs a clock-in or clock-out event within the DJT platform.
- **Continuous/background tracking:** DJT does not collect continuous background location data outside of specific clock-in/out actions.
- **Who can access:** Authorized business administrators within the same tenant may access attendance and location records for their employees.
- **Purpose:** Location is used to verify workforce attendance, support scheduling accuracy, and operate the timekeeping feature.
- **Retention:** Location records are retained as part of attendance history according to DJT's data retention practices.

Customers using location features are responsible for providing legally required notices to their employees, obtaining required consents, and using location data only for legitimate workforce management purposes consistent with applicable law. DJT prohibits using location features for unlawful employee surveillance or monitoring outside the intended business purpose.

11. Communications Privacy — Phone, SMS, WhatsApp & Email

DJT supports business communications through multiple channels:

Phone & AI Phone Agents

DJT provides AI-powered phone handling through Telnyx. Where call recording or transcription is enabled, DJT may generate call logs, recordings, transcripts, and AI summaries. Customers are responsible for obtaining legally required recording consent from call participants in their jurisdiction. DJT provides tools that may assist with disclosure; those tools do not transfer all legal recording responsibility to DJT.

SMS

DJT may send or receive SMS messages through authorized carrier infrastructure. Customers using SMS features must comply with applicable messaging laws and consent requirements.

WhatsApp

DJT may provide WhatsApp integration where customers connect a WhatsApp Business account. Message metadata and content within authorized scopes may be processed. Customers must comply with WhatsApp platform policies and applicable messaging consent requirements.

Email Integration

When customers connect Gmail or Microsoft 365, DJT accesses email and calendar data within authorized OAuth scopes. Email content processed through DJT is used to provide requested automation, AI, and communication features. DJT does not use your email content for advertising or cross-customer analysis.

DJT does not claim responsibility for all legal consent requirements applicable to your use of communications features. You remain responsible for ensuring your communications practices comply with applicable law in your jurisdiction.

12. Payment & Billing Information

DJT processes billing information to manage subscriptions, DJT Credits, invoices, and refunds. Payment card processing is handled by authorized payment providers (Stripe, Flutterwave). DJT receives payment event notifications and identifiers but does not store complete payment card numbers. M-Pesa and Wise payment information is processed through respective provider infrastructure.

DJT maintains transaction history, invoice records, Credit ledgers, payment status, and refund/dispute records for accounting, customer service, and fraud prevention purposes.

13. Support & Refund Evidence

When you submit a support ticket, refund claim, or privacy request, DJT collects the information you provide including descriptions, screenshots, uploaded files, error references, and communications. This information is used to investigate and resolve your request.

DJT stores support evidence securely and limits access to authorized DJT staff. Customers submitting support evidence should not include passwords, private API keys, authentication codes, full payment card numbers, or sensitive personal information unrelated to the support issue.

14. How We Use Your Information

DJT uses information for the following purposes:

- Operating and delivering DJT platform services, including Atlas, Business Memory, Pulse, payroll tools, communications, and all other subscribed features.
- Authenticating users and managing tenant access.
- Operating AI-powered features, including processing prompts and Business Memory through authorized AI infrastructure.
- Processing communications, phone calls, email, SMS, and WhatsApp where connected.
- Supporting workforce management, timekeeping, and payroll workflows.
- Providing integrations with connected third-party services.
- Processing payments, managing subscriptions, and maintaining Credit accounts.

- Responding to support tickets, refund claims, and privacy requests.
- Preventing fraud, abuse, and unauthorized access.
- Monitoring security events, maintaining audit logs, and protecting DJT infrastructure.
- Troubleshooting technical issues and improving platform reliability.
- Complying with legal obligations, responding to lawful requests, and cooperating with law enforcement where required.
- Improving legitimate platform functionality on an aggregated, non-identifying basis where possible.

DJT does not use customer Business Memory, employee records, or private communication content for advertising, marketing, or cross-customer analytics. DJT's purpose is to operate the software you have paid for, not to monetize your data.

15. How We Share Information

DJT shares information only in the following circumstances:

- With authorized DJT service providers and subprocessors (see Section 16) who process information on DJT's behalf to deliver platform services.
- With third-party services you connect to DJT (Google, Microsoft, Telnyx, Stripe, Flutterwave, etc.) — only within the scopes you authorize.
- With lawful authorities when required by applicable law, court order, or legal process.
- In connection with a merger, acquisition, or sale of DJT assets, where the recipient is bound by appropriate confidentiality obligations.
- To protect DJT, other customers, or third parties from fraud, abuse, illegal activity, or security threats.
- With your authorization or at your direction.

DJT does not sell customer information. DJT does not share customer Business Memory, employee records, or communication content for advertising, marketing, or behavioral profiling purposes.

16. Third-Party Service Providers & Subprocessors

DJT uses trusted third-party providers to operate the platform. These providers process data on DJT's behalf under appropriate agreements. Categories and known providers include:

Database & Hosting	Supabase (database, authentication, storage), Vercel (hosting/edge), Cloudflare (network, security, DNS)
AI / Model Infrastructure	Anthropic (Claude AI models), OpenAI (AI models) — requests are processed to generate AI responses
Payments	Stripe (subscription billing, payment processing), Flutterwave (Africa payments), M-Pesa infrastructure (Kenya mobile payments), Wise (international transfers)
Telecom / Communications	Telnyx (phone, SMS, call routing, AI voice)
Email & Calendar	Google (Gmail integration), Microsoft (Microsoft 365 / Outlook integration)
Messaging	Meta / WhatsApp Business API
Authentication	Supabase Auth (primary authentication)
Error & Performance	Internal logging and monitoring infrastructure

DJT maintains a current list of authorized subprocessors. If you require a complete subprocessor list, please contact hello@dahnjay.tech

17. Selling Customer Data

DJT's business model is to provide software and services to customers — not to sell customer data. DJT does not sell customer business data, employee records, communication content, or Business Memory for monetary consideration to third parties.

DJT does not use advertising tracking pixels, behavioral advertising SDKs, cross-context behavioral advertising, or marketing data broker arrangements as of this version of the Privacy Policy. If this changes in the future, this policy will be updated before any such use begins.

18. Children & Minors

DJT is a B2B platform intended for adult business users. DJT business accounts are intended for users who are at least 18 years old or who have legal authority to enter into agreements on behalf of their organization. DJT does not knowingly provide business accounts to minors acting independently.

DJT is not directed at children as a consumer service. DJT does not knowingly collect personal information directly from children under 13 (or a higher age threshold under applicable law) as end-users of the platform.

Businesses that provide services to, employ, supervise, or otherwise process information involving individuals under 18 have additional privacy and legal obligations under applicable law. Those businesses are responsible for complying with such obligations. During DJT onboarding, businesses declare whether their operations involve minors so that DJT can maintain appropriate records.

19. International Data Processing

DJT serves customers in the United States, Kenya, and other markets. DJT uses service providers that may operate data centers and process information in countries other than the customer’s country of residence or incorporation.

By using DJT services, you acknowledge that information may be processed internationally where DJT’s service providers operate, subject to applicable data protection safeguards. DJT selects providers based in part on their data protection commitments.

[ATTORNEY DECISION REQUIRED] Jurisdiction-specific international transfer mechanisms (Standard Contractual Clauses, adequacy determinations, or equivalents applicable to Kenya and the US) must be reviewed and confirmed by legal counsel before publication of this section.

20. Data Retention

DJT retains information for as long as reasonably necessary to:

- Provide active DJT services to the account.
- Meet applicable legal, accounting, tax, and regulatory requirements.
- Prevent fraud and maintain platform security.
- Resolve active support, refund, or dispute cases.
- Comply with legal hold or investigation requirements.
- Expire through backup and archival cycles.

Retention periods vary by data category. High-sensitivity categories deserve particular attention:

GPS/Location records	Retained as part of attendance history for the active tenancy period. Review scheduled post-launch.
Call recordings & transcripts	Retained for business use and support reference. Duration subject to customer configuration and legal review.
Payroll data	Retained per applicable legal requirements (US and Kenya). Specific periods require legal review.
Support evidence	Retained for dispute resolution, refund processes, and legal hold periods.
Security/audit logs	Retained for security and fraud investigation purposes.
Deleted tenant data	Account closure initiates a data handling process; some information is retained per legal obligations before permanent deletion.

[ATTORNEY DECISION REQUIRED] Specific legally required retention periods for US and Kenya payroll records, employment data, communications, and financial records must be confirmed by legal counsel before specific durations are published.

21. Your Privacy Rights

Depending on your location and applicable law, you may have the following rights with respect to your information:

Access	Request a summary of the information DJT holds about you or your account.
Correction	Request correction of inaccurate or incomplete information.
Deletion	Request deletion of your personal information, subject to legal retention requirements.
Portability / Export	Request an export of your data in a usable format where technically available.
Objection / Restriction	Object to or request restriction of certain processing activities, where applicable law supports this.
Withdraw Consent	Where processing is based on consent, withdraw consent (this does not affect prior processing).
Complaint	Lodge a complaint with a relevant regulatory authority in your jurisdiction.

Not all rights apply in every jurisdiction. DJT will respond to verifiable requests within a reasonable timeframe. DJT may need to verify your identity and account authority before processing requests. For employee information submitted by an employer-customer, requests may need to be directed through the employing organization.

[ATTORNEY DECISION REQUIRED] Specific rights, timelines, and response requirements under applicable US state laws (e.g. CCPA/CPRA) and Kenya's Data Protection Act must be confirmed by legal counsel before publication.

22. How to Submit a Privacy Request

Privacy requests may be submitted through the following channels:

- Authenticated DJT Account: dashboard !' Account Settings !' Privacy & Data !' Submit Request.
- Email: hello@dahnjay.tech — use subject line "Privacy Request" from the email address registered to your DJT account.

DJT will acknowledge receipt of your request and respond within a reasonable time. For requests involving account or data deletion, DJT will verify your identity and account authority. DJT will not automatically perform destructive actions based on unauthenticated requests.

Types of requests DJT processes: data export, data correction, account/tenant deletion, privacy questions, and other applicable rights requests. DJT maintains an internal Privacy Request queue for admin review and tracking.

23. Security

DJT uses reasonable administrative, technical, and organizational safeguards designed to protect information from unauthorized access, disclosure, alteration, and destruction. Our security measures include:

- Authentication with multi-factor authentication (MFA) support.
- Row-Level Security (RLS) on the database to enforce tenant isolation.
- Encrypted storage and transmission of sensitive credentials.
- Audit logging of security events and administrative actions.
- Webhook signature verification for provider integrations.
- Role-based access controls limiting staff access to necessary systems.
- Vendor security requirements for authorized subprocessors.

No security system is perfectly impenetrable. DJT does not claim to be "100% secure," "unhackable," or immune to all possible breaches. DJT works to maintain reasonable and appropriate security controls consistent with industry practices.

24. Security Incidents

If DJT becomes aware of a security incident affecting customer information, DJT will take reasonable steps to investigate and contain the incident, assess the scope and severity, implement remediation measures, and provide required notifications to affected customers and/or regulatory authorities where legally required by applicable law.

DJT maintains internal incident response procedures. The details of those procedures are not published in order to maintain their effectiveness. DJT does not expose sensitive security detection or response logic in customer-facing documentation.

25. Cookies & Browser Storage

DJT uses essential cookies and browser storage mechanisms to operate the platform:

- Authentication cookies and session tokens — required to maintain your logged-in session. Without these, the platform cannot function.
- Local storage — used to store user preferences and application state within your browser.
- Session storage — used for temporary session data within a single browsing session.

As of the date of this policy, DJT does not use analytics cookies, advertising cookies, tracking pixels, behavioral advertising SDKs, session-replay tools, or third-party marketing tracking. If DJT introduces any such tracking in the future, this policy will be updated and, where required, customer consent will be obtained.

Essential security and session cookies cannot be disabled without preventing platform access. No consent banner is required for strictly necessary cookies under applicable law in most jurisdictions. DJT will assess cookie consent requirements based on applicable law and any future non-essential cookies introduced.

26. Changes to This Privacy Policy

DJT may update this Privacy Policy from time to time. When we make material changes, we will notify customers through the DJT dashboard or via registered email. The effective date at the top of this policy reflects when the current version took effect. Prior versions are retained in DJT's legal versioning system and are available upon request.

Continued use of DJT following a policy update constitutes acknowledgement of the updated policy. For changes that require renewed consent, DJT will request it where legally required.

27. Contact & Privacy Inquiries

For privacy questions, requests, or concerns:

Email: hello@dahnjay.tech (subject: "Privacy Request" or "Privacy Inquiry")
Website: dahnjay.tech
DJT Platform: Dashboard !' Account Settings !' Privacy & Data

DJT will respond to privacy inquiries in a timely manner. If you are located in a jurisdiction with a supervisory authority for data protection, you may also have the right to lodge a complaint with that authority if you believe your privacy rights have been violated. DJT encourages you to contact us first so we can attempt to resolve your concern directly.