TALENT PRO

Privacy Policy

Walumo

Version: 3.0

Last Updated: June 2026

1. Introduction

Walumo is committed to protecting the privacy, confidentiality, and personal data of all users of the Talent Pro platform.

This Privacy Policy explains how Walumo collects, uses, stores, shares, protects, transfers, and deletes personal data when users access or use Talent Pro.

This Policy applies to:

1. Candidates;
2. Recruiters;
3. Hiring managers;
4. Employers;
5. Company administrators;
6. Freelancers;
7. Training participants;
8. LMS learners;
9. Community users;
10. Visitors to Talent Pro websites;
11. Users of Talent Pro mobile applications;
12. Users of AI-powered Talent Pro features.

Talent Pro may be accessed through:

1. A website;
2. A web application;
3. A mobile application;
4. An admin portal;
5. APIs;
6. Email communications;
7. Third-party integrations;
8. AI-powered tools and workflows.

This Policy should be read together with:

1. Talent Pro Terms and Conditions;
2. Talent Pro Cookie and Tracking Technologies Policy;
3. Talent Pro AI Terms;
4. Talent Pro Data Processing Addendum;
5. Any customer-specific agreement;
6. Any country-specific privacy notice that may apply.

Where local law gives users stronger rights than this Policy, Walumo will apply the stronger legal standard.

2. Who We Are

Talent Pro is developed and operated by **Walumo**.

For purposes of data protection law, Walumo may act as:

1. A **data controller**, where Walumo decides why and how personal data is processed.
2. A **data processor**, where Walumo processes personal data on behalf of a client, employer, recruitment agency, or organization.
3. A **joint controller**, where Walumo and another organization jointly determine certain processing purposes, depending on the arrangement.

Where Talent Pro is used by an employer, recruitment agency, or client organization, that organization may also be responsible for how it uses candidate, employee, applicant, recruiter, or freelancer data.

3. Scope of This Policy

This Policy covers personal data processed through Talent Pro, including data collected directly from users, generated through platform use, received from recruiters or employers, created by AI systems, obtained from third-party integrations, or collected through cookies and similar technologies.

This Policy does not replace the privacy policies of third-party service providers, payment providers, social login providers, app stores, or employer/recruiter organizations that may separately process user data.

4. Definitions

For clarity, the following terms apply:

Personal Data means any information that identifies, relates to, describes, or can reasonably be linked to an individual.

Sensitive Personal Data means personal data that receives special protection under applicable law. This may include health data, disability information, biometric data, racial or ethnic origin, religious beliefs, political opinions, trade union membership, criminal history, government identifiers, precise location data, financial account data, or other legally protected information.

Processing means any action performed on personal data, including collection, storage, use, sharing, analysis, deletion, transfer, or anonymization.

Candidate means a user who creates a profile, applies for jobs, uses career tools, takes training, participates in AI coaching, or uses Talent Pro for professional opportunities.

Recruiter means a user who posts jobs, reviews candidates, manages pipelines, communicates with applicants, evaluates profiles, or manages recruitment workflows.

AI Features means artificial intelligence-powered tools used for matching, recommendations, coaching, CV analysis, cover letter support, interview simulation, profile improvement, skill gap analysis, or recruiter support.

Anonymized Data means data that can no longer reasonably identify an individual.

Pseudonymized Data means data that does not directly identify a person without additional information but may still be personal data under applicable law.

5. Personal Data We Collect

Talent Pro may collect the following categories of personal data.

5.1 Identification and Account Data

We may collect:

1. First name;
2. Last name;
3. Username;
4. Email address;
5. Telephone number;
6. Country;
7. City;
8. Profile picture;
9. Account login credentials;
10. Authentication method;
11. Account status;
12. User role;
13. Organization or company affiliation;
14. User ID;
15. Internal account reference number.

Purpose:

1. To create and manage user accounts;
2. To authenticate users;
3. To provide platform access;
4. To support account security;
5. To communicate with users;
6. To assign correct access levels.

5.2 Candidate Profile Data

We may collect:

1. Professional title;
2. Biography;
3. Career summary;
4. Work preferences;
5. Remote, hybrid, or in-person preference;
6. Preferred job locations;
7. Availability;
8. Salary expectations;
9. Desired role;
10. Employment status;
11. Skills;
12. Languages and proficiency levels;
13. Professional interests;
14. Portfolio links;
15. Public professional profiles;
16. Career goals.

Purpose:

1. To build candidate profiles;
2. To support job matching;
3. To recommend opportunities;
4. To help recruiters assess candidate suitability;
5. To personalize platform experience.

5.3 Professional and Recruitment Data

We may collect:

1. CVs;
2. Résumés;
3. Cover letters;
4. Employment history;
5. Education history;
6. Degrees;
7. Certifications;
8. Licenses;
9. Professional references;
10. Project history;
11. Portfolio documents;
12. Work samples;
13. Interview notes;
14. Recruiter evaluations;
15. Application status;
16. Candidate pipeline stage;

17. Recruiter comments;
18. Internal notes;
19. Application history;
20. Candidate shortlisting status;
21. Rejection or progression status;
22. Interview availability;
23. Candidate assessment responses.

Purpose:

1. To manage recruitment workflows;
2. To allow candidates to apply for roles;
3. To allow recruiters to review applications;
4. To support interviews and selection processes;
5. To track recruitment pipeline progress;
6. To provide recruitment reporting and analytics.

5.4 Application and Assessment Data

We may collect:

1. Answers to recruiter questions;
2. Screening responses;
3. Interview responses;
4. Assessment results;
5. Test scores;
6. Candidate rankings;
7. Matching scores;
8. Recruiter feedback;
9. Hiring manager feedback;
10. Application decisions;
11. Application timestamps;
12. Pipeline activity;
13. Status changes;
14. Candidate communication history.

Purpose:

1. To manage applications;
2. To evaluate candidate suitability;
3. To support recruiter and employer decisions;
4. To improve recruitment workflows;
5. To provide audit trails and accountability.

5.5 Training and Learning Management Data

Where Talent Pro includes learning, training, bootcamp, or LMS features, we may collect:

1. Courses enrolled in;
2. Lessons completed;
3. Progress data;
4. Quiz scores;
5. Assessment results;
6. Certificates issued;
7. Certificate dates;
8. Bootcamp participation;
9. Cohort membership;
10. Attendance records;
11. Learning activity logs;
12. Instructor feedback.

Purpose:

1. To provide training services;
2. To track course progress;
3. To issue certificates;
4. To recommend learning paths;
5. To support career development;
6. To report learner performance where appropriate.

5.6 Freelance and Project Data

Where Talent Pro includes freelance or project marketplace features, we may collect:

1. Project proposals;
2. Freelancer profiles;
3. Project applications;
4. Active contracts;
5. Project milestones;
6. Deliverables;
7. Client feedback;
8. Work history;
9. Project status;
10. Completion records;
11. Payment requests;
12. Dispute records;
13. Ratings and reviews.

Purpose:

1. To connect freelancers with clients;
2. To manage project delivery;

3. To track milestones;
4. To process payments;
5. To support dispute resolution;
6. To maintain freelancer work history.

5.7 Financial and Payment Data

Where payments, subscriptions, wallets, tokens, payouts, or paid services are enabled, we may collect:

1. Wallet balance;
2. Subscription status;
3. Payment method type;
4. Payment provider reference;
5. Transaction history;
6. Payout requests;
7. Refund requests;
8. Billing details;
9. Invoice information;
10. Tax-related records;
11. Currency;
12. Payment status;
13. AI token purchases;
14. Premium feature usage;
15. Fraud prevention information.

Talent Pro does not intentionally store full card numbers where payments are handled by regulated payment providers.

Purpose:

1. To process payments;
2. To manage subscriptions;
3. To process payouts;
4. To issue invoices;
5. To prevent fraud;
6. To comply with accounting, tax, and legal obligations.

5.8 AI-Generated and AI-Processed Data

Talent Pro may process data through AI-powered features.

This may include:

1. Profile embeddings;

2. Vector representations of candidate profiles;
3. AI-generated career summaries;
4. AI-generated CV analysis;
5. AI-generated cover letter drafts;
6. AI-generated interview preparation content;
7. AI-generated coaching feedback;
8. AI-generated skill gap analysis;
9. AI-generated salary insights;
10. AI-generated candidate match scores;
11. AI-generated job recommendations;
12. AI-generated recruiter summaries;
13. AI conversation history;
14. Simulated interview history;
15. AI usage logs;
16. AI token consumption;
17. AI prompt and response metadata;
18. AI feedback submitted by users.

Purpose:

1. To support candidate matching;
2. To recommend jobs;
3. To help candidates improve profiles;
4. To provide career coaching;
5. To assist with interview preparation;
6. To help recruiters review information more efficiently;
7. To improve user experience;
8. To monitor AI quality and safety;
9. To detect misuse or abuse.

5.9 Messaging and Communication Data

We may collect:

1. Messages between candidates and recruiters;
2. Messages between freelancers and clients;
3. System notifications;
4. Interview invitations;
5. Email delivery records;
6. Email open and click data where enabled;

7. Message timestamps;
8. Message status;
9. Attachments shared in messages;
10. Support communications;
11. Feedback submitted to Walumo;
12. Complaint records.

Purpose:

1. To enable communication;
2. To support recruitment workflows;
3. To provide notifications;
4. To maintain communication history;
5. To provide user support;
6. To investigate abuse, fraud, or policy violations.

5.10 Community Data

Where community features are enabled, we may collect:

1. Posts;
2. Comments;
3. Reactions;
4. Groups joined;
5. Community activity;
6. Profile visibility settings;
7. Reports of inappropriate content;
8. Moderation records.

Purpose:

1. To operate community spaces;
2. To allow professional interaction;
3. To moderate content;
4. To enforce community rules;
5. To prevent abuse.

5.11 Device, Connection, Log, and Security Data

We may collect:

1. IP address;
2. Browser type;
3. Device type;
4. Operating system;

5. App version;
6. Device identifiers;
7. Session identifiers;
8. Login timestamps;
9. Pages viewed;
10. Actions performed;
11. Session duration;
12. Error logs;
13. Crash logs;
14. Authentication logs;
15. Security logs;
16. Audit logs;
17. WebSocket connection data;
18. Cookies and similar technologies;
19. Approximate location derived from IP address;
20. Suspicious activity signals.

Purpose:

1. To secure the platform;
2. To detect fraud;
3. To prevent unauthorized access;
4. To monitor system performance;
5. To improve reliability;
6. To troubleshoot errors;
7. To comply with audit requirements.

5.12 Mobile App Data

If users access Talent Pro through iOS or Android applications, we may collect:

1. App instance ID;
2. Device model;
3. Operating system version;
4. App version;
5. Push notification token;
6. Crash logs;
7. Diagnostic data;

8. Mobile permissions used by the app;
9. File upload metadata;
10. Camera or photo access, where user permits;
11. Microphone access, where voice or interview features are enabled and user permits;
12. Device language;
13. Device region;
14. Mobile authentication data;
15. Payment SDK data;
16. Analytics SDK data, where enabled.

Purpose:

1. To operate the mobile app;
2. To provide notifications;
3. To allow file uploads;
4. To support interviews and media uploads;
5. To diagnose crashes;
6. To meet app store privacy requirements.

5.13 Sensitive Personal Data

Talent Pro does not intentionally request sensitive personal data unless it is necessary, lawful, and clearly explained.

However, sensitive personal data may appear in:

1. CVs;
2. Cover letters;
3. Interview responses;
4. Candidate messages;
5. Recruiter notes;

6. Uploaded documents;
7. Disability accommodation requests;
8. Equal opportunity monitoring, where enabled;
9. Background check workflows, where legally permitted;
10. Health or safety-related employment documents, where required by law.

Users should avoid uploading sensitive personal data unless it is necessary for a specific recruitment, employment, legal, accessibility, or platform purpose.

Where sensitive personal data is required, Walumo will apply additional safeguards and will rely on an appropriate legal basis under applicable law.

6. How We Collect Personal Data

Walumo may collect personal data from:

1. Users directly;
2. Candidate profile forms;
3. Uploaded CVs and documents;
4. Job applications;
5. Recruiter dashboards;
6. Employer or client organizations;
7. Training and LMS activity;
8. Freelance project activity;
9. Messaging and community features;
10. AI-powered tools;
11. Cookies and similar technologies;
12. Mobile applications;
13. Payment providers;
14. Authentication providers;
15. Support requests;
16. Publicly available professional information, where lawful;
17. Third-party integrations selected or authorized by the user.

7. Why We Process Personal Data

Walumo processes personal data for the purposes below.

7.1 Account Creation and Platform Access

We process personal data to:

1. Create user accounts;

2. Verify user identity;
3. Authenticate users;
4. Manage login sessions;
5. Assign user roles;
6. Provide secure access;
7. Maintain user profiles.

7.2 Recruitment and Application Management

We process personal data to:

1. Allow candidates to apply for jobs;
2. Allow recruiters to post jobs;
3. Allow recruiters to manage applications;
4. Track recruitment stages;
5. Send interview invitations;
6. Share candidate profiles with relevant recruiters or employers;
7. Support shortlisting;
8. Support hiring workflows;
9. Maintain recruitment records.

7.3 AI Matching, Recommendations, and Career Support

We process personal data to:

1. Match candidates with suitable opportunities;
2. Recommend jobs;
3. Recommend candidates to recruiters;
4. Calculate profile strength;
5. Analyse CVs;
6. Generate cover letter drafts;
7. Provide career coaching;
8. Simulate interviews;
9. Identify skills gaps;
10. Provide salary insights;
11. Improve candidate readiness;
12. Support recruiter productivity.

AI outputs are intended to assist users and recruiters. They should not be treated as the sole basis for hiring, rejection, compensation, promotion, or other legally significant decisions.

7.4 Training and Learning Management

We process training data to:

1. Deliver courses;
2. Track learning progress;
3. Issue certificates;
4. Manage cohorts;
5. Recommend courses;
6. Evaluate training effectiveness;
7. Support learner development.

7.5 Freelance and Contract Management

We process freelance data to:

1. Connect freelancers and clients;
2. Manage proposals;
3. Track contracts;
4. Manage milestones;
5. Confirm deliverables;
6. Process payments;
7. Resolve disputes;
8. Maintain project history.

7.6 Payments, Billing, Wallets, and Subscriptions

We process financial and payment data to:

1. Process payments;
2. Manage subscriptions;
3. Maintain wallet balances;
4. Process payouts;
5. Process refunds;
6. Issue invoices;
7. Detect payment fraud;
8. Comply with accounting, tax, and financial obligations.

7.7 Communication and Notifications

We process contact and communication data to:

1. Send account notifications;
2. Send application updates;
3. Send recruiter messages;
4. Send interview invitations;
5. Send training updates;
6. Send payment confirmations;
7. Send security alerts;
8. Send support responses;
9. Send marketing messages where the user has consented or where lawful.

7.8 Platform Improvement and Analytics

We process usage data to:

1. Improve platform design;
2. Improve user experience;
3. Identify bugs;
4. Monitor system performance;
5. Understand feature adoption;
6. Improve onboarding;
7. Improve AI safety and quality;
8. Generate aggregated business insights;
9. Support product development.

Where required by law, analytics cookies or similar technologies will only be used with user consent.

7.9 Security, Fraud Prevention, and Legal Compliance

We process data to:

1. Protect accounts;
2. Prevent unauthorized access;
3. Detect fraud;
4. Prevent abuse;
5. Monitor suspicious activity;
6. Enforce Terms and Conditions;
7. Respond to legal requests;
8. Maintain audit logs;

9. Comply with laws and regulations;
10. Protect users, clients, Walumo, and the public.

8. Legal Bases for Processing

Depending on the user's location and the purpose of processing, Walumo may rely on one or more of the following legal bases.

We process data where necessary to provide Talent Pro services requested by the user or agreed with a client.

Examples:

1. Creating an account;
2. Managing applications;
3. Providing recruiter access;
4. Enabling messaging;
5. Processing subscriptions;
6. Providing training;
7. Managing freelance contracts.

8.2 Consent

We rely on consent where required by law or where the user has a real choice.

Examples:

1. Optional marketing communications;
2. Non-essential cookies;
3. Optional analytics in consent-based jurisdictions;
4. Certain AI features where consent is required;
5. Certain mobile app permissions;
6. Use of sensitive personal data where explicit consent is legally required;
7. Optional public profile visibility;
8. Optional community participation.

Users may withdraw consent at any time. Withdrawal does not affect processing that occurred before consent was withdrawn.

8.3 Legitimate Interests

We may rely on legitimate interests where the processing is necessary, proportionate, and does not override user rights.

Examples:

1. Platform security;
2. Fraud prevention;
3. Product improvement;
4. Internal reporting;
5. Error detection;
6. Service analytics where lawful;
7. Preventing misuse;
8. Maintaining audit logs;
9. Communicating service-related updates;
10. Improving recruitment workflows.

Users may object to processing based on legitimate interests where applicable.

8.4 Legal Obligations

We process data where necessary to comply with legal obligations.

Examples:

1. Accounting records;
2. Tax records;
3. Regulatory compliance;
4. Employment-related obligations;
5. Anti-fraud obligations;
6. Responding to lawful authority requests;
7. Recordkeeping obligations;
8. Data protection obligations.

8.5 Vital Interests

In limited circumstances, we may process personal data to protect someone's life, health, or safety.

8.6 Public Interest or Official Authority

Where applicable, certain processing may be carried out in the public interest or under official authority, but only legally supported.

9. Artificial Intelligence and Automated Processing

Talent Pro uses AI to support recruitment, candidate development, recruiter productivity, and career guidance.

AI features may include:

1. Candidate-job matching;
2. Profile strength scoring;
3. CV analysis;
4. Cover letter generation;
5. Career coaching;
6. Interview preparation;
7. Simulated interviews;

8. Skills gap analysis;
9. Salary insights;
10. Recruiter summaries;
11. Candidate recommendations;
12. Job recommendations;
13. AI-generated communication support.

9.1 No Solely Automated Hiring Decision

Talent Pro does not intend for hiring, rejection, employment, promotion, compensation, or legally significant decisions to be made solely by AI.

AI-generated scores, rankings, summaries, or recommendations are decision-support tools.

Recruiters, employers, and hiring managers remain responsible for human review and final decisions.

9.2 Human Review

Users may request human review of an AI-assisted assessment, match score, recommendation, or automated output where applicable.

Requests may be sent to the Walumo data protection contact listed in this Policy.

9.3 AI Fairness and Bias Control

Walumo aims to apply appropriate safeguards to AI systems, including:

1. Human oversight;
2. Testing for unfair bias;
3. Data quality controls;
4. Monitoring of AI outputs;
5. Logging of AI system activity;
6. Review of high-impact AI features;
7. Clear user-facing explanations;
8. Restriction of inappropriate data use;
9. Security controls;
10. Vendor review.

9.4 AI Providers

Talent Pro may use internal and external AI systems.

These may include:

1. Walumo internal AI systems;
2. OpenAI;
3. Anthropic;
4. Other approved AI infrastructure providers.

Where external providers are used, data may be transmitted to those providers to deliver the requested AI feature. Walumo will apply contractual, technical, and organizational safeguards appropriate to the risk.

9.5 AI and Recruitment Compliance

Because AI in recruitment can affect professional opportunities, Talent Pro treats AI recruitment functionality as a higher-risk area requiring stronger governance.

This may include:

1. AI system documentation;
2. Human oversight;
3. Audit trails;
4. Bias monitoring;
5. Clear explanations to users;
6. Limiting sensitive data use;
7. Vendor due diligence;
8. Security controls;
9. Escalation processes;
10. Legal review before major AI releases.

10. Data Sharing and Recipients

Walumo may share personal data only where necessary for the purposes described in this Policy.

10.1 Internal Walumo Teams

Data may be accessed by authorized Walumo personnel, including:

1. Product teams;
2. Engineering teams;
3. Customer support;
4. Security teams;
5. Legal and compliance teams;
6. Operations teams;
7. Finance teams, where payments are involved.

Access is limited based on role and need.

10.2 Recruiters, Employers, and Hiring Organizations

Candidate profile and application data may be shared with recruiters, employers, recruitment agencies, or hiring organizations when:

1. A candidate applies for a job;
2. A candidate chooses to make a profile visible;
3. A recruiter is authorized to access the candidate's profile;
4. A client organization uses Talent Pro for recruitment;
5. Sharing is necessary for the recruitment process.

Recruiters and employers are responsible for how they use candidate data within their own hiring processes.

10.3 Training Providers and Instructors

Where LMS or training features are enabled, data may be shared with authorized instructors, trainers, cohort managers, or training partners to deliver courses and issue certificates.

10.4 Freelance Clients and Project Participants

Where freelance features are enabled, relevant profile, proposal, contract, milestone, deliverable, and payment data may be shared with clients or freelancers involved in the project.

10.5 Service Providers

Walumo may use trusted service providers to support Talent Pro.

These may include:

Provider / Category	Purpose
Microsoft Azure	Hosting, file storage, infrastructure, backups, security, and platform availability
SendGrid or equivalent	Transactional emails, registration confirmations, application updates, interview invitations, and service notifications
OpenAI	AI-powered features such as embeddings, content support, recommendations, or fallback AI capabilities
Anthropic	AI-powered features such as coaching, CV support, interview preparation, and profile analysis
Payment providers such as Paystack, Flutterwave, Stripe, M-Pesa, or Safaricom	Payments, payouts, subscriptions, refunds, billing, fraud prevention, and transaction records
Authentication providers such as Google, LinkedIn, or Microsoft	User login and identity verification where enabled
Analytics and diagnostics providers	Product analytics, crash reporting, error monitoring, and performance improvement where enabled
Security providers	Threat detection, fraud prevention, access control, and account protection

Service providers may process data only for approved purposes and under appropriate confidentiality, security, and data protection obligations.

10.6 Legal, Regulatory, and Safety Disclosures

Walumo may disclose data where necessary to:

1. Comply with law;
2. Respond to lawful requests;
3. Protect user safety;
4. Protect platform security;
5. Enforce Terms and Conditions;
6. Investigate fraud;
7. Protect Walumo's rights;
8. Resolve disputes;
9. Support audits;

10. Comply with court orders or regulator requests.

10.7 No Sale of Personal Data

Walumo does not sell personal data in the ordinary meaning of selling personal data for money.

If any future activity is considered a "sale," "sharing," or "targeted advertising" under applicable privacy laws, Walumo will provide the required notices and opt-out rights.

11. International Data Transfers

Talent Pro may operate across multiple countries. Personal data may be processed in countries where Walumo, its clients, partners, affiliates, or service providers operate.

This may include:

1. Democratic Republic of Congo;
2. Kenya;
3. Rwanda;
4. Tanzania;
5. Uganda;
6. Zambia;
7. South Africa;
8. Nigeria;
9. United States;
10. European Union or European Economic Area countries;
11. United Kingdom;
12. Other countries where Talent Pro operates or service providers are located.

Where data is transferred internationally, Walumo will apply appropriate safeguards, which may include:

1. Data processing agreements;
2. Standard contractual clauses;
3. Adequacy decisions where available;
4. Transfer risk assessments;
5. Encryption;
6. Access controls;
7. Vendor due diligence;
8. Data minimization;
9. Regional hosting where required;
10. Contractual confidentiality obligations.

12. Data Security

Walumo applies technical and organizational security measures designed to protect personal data against unauthorized access, loss, misuse, alteration, disclosure, or destruction.

Security measures may include:

1. HTTPS/TLS encryption in transit;
2. Encryption at rest where appropriate;
3. Access control by user role;
4. Multi-organization data separation;
5. JWT authentication with short-lived access tokens;
6. Refresh token controls;
7. Two-factor authentication where enabled;
8. Secure password handling;
9. Audit logs for sensitive actions;
10. Secure file storage;
11. Regular backups;
12. Vulnerability management;
13. Monitoring for suspicious activity;
14. Incident response procedures;
15. Vendor security review;
16. Secure development practices;
17. Logging and traceability;
18. Least-privilege access control.

No system is completely secure. Users are responsible for keeping their account credentials confidential and notifying Walumo of suspected unauthorized access.

13. Data Retention

Walumo retains personal data only for as long as necessary for the purposes described in this Policy, unless a longer retention period is required by law, contract, audit, security, dispute resolution, or regulatory obligation.

Data Category	Typical Retention Period	Reason
Active candidate profile	Account lifespan	Provision of Talent Pro services
Inactive account data	Up to 24 months after last activity unless deletion is requested earlier	Account reactivation, service continuity, compliance

Job applications	Up to 2 years after last recruitment activity, unless client settings or law require otherwise	Recruitment follow-up and audit trail
Recruiter notes and evaluations	Up to 2 years after last activity, unless law or client policy requires otherwise	Recruitment accountability
Messages and conversations	Up to 2 years after last activity	Communication history and dispute resolution
Training progress and certificates	Account lifespan or longer where certificates must remain verifiable	Training history and certification
Freelance contracts and deliverables	Up to 7 years where payment, tax, or contract records are involved	Contract, accounting, tax, and dispute purposes
Payment and transaction records	Up to 7 years or longer if required by law	Accounting, tax, financial compliance
Security and audit logs	Up to 12 months, unless needed longer for investigation	Security and fraud prevention
AI embeddings and profile vectors	Account lifespan or until account deletion, unless anonymized	Matching and recommendations
AI coaching and simulated interview history	Up to 24 months or until deletion request, subject to legal exceptions	User experience and service continuity
Cookie consent records	Up to 12 months or legally required period	Consent accountability
Marketing consent records	Until withdrawn, plus a reasonable suppression period	Consent and opt-out management
Community content	Account lifespan or until deleted/moderated	Community participation
Deleted account data	Deleted from active systems within 30 days, subject to legal exceptions	Account deletion
Backups	Deleted according to backup rotation schedule	Security and disaster recovery

Anonymized and aggregated data may be retained for longer where it can no longer reasonably identify an individual.

14. Account Deletion

Users may request deletion of their account through:

Settings → Privacy → Delete My Account

or by contacting Walumo through the contact details in this Policy.

After a valid deletion request:

1. Walumo will begin deletion within a reasonable period.
2. Active profile data will generally be deleted within 30 days.
3. Some data may remain in backups until backup cycles complete.
4. Financial, tax, legal, security, dispute, or audit records may be retained where required.
5. Anonymized or aggregated data may be retained.
6. Data controlled by recruiters, employers, or third-party providers may be subject to their own deletion processes.

15. User Rights

Depending on the user's location and applicable law, users may have the following rights.

15.1 Right to Be Informed

Users have the right to understand how their personal data is collected, used, shared, retained, and protected.

15.2 Right of Access

Users may request access to personal data held about them.

15.3 Right to Rectification

Users may request correction of inaccurate or incomplete personal data.

15.4 Right to Erasure

Users may request deletion of personal data where applicable.

15.5 Right to Restrict Processing

Users may request restriction of processing in certain circumstances.

15.6 Right to Object

Users may object to processing based on legitimate interests or direct marketing.

15.7 Right to Data Portability

Users may request a copy of their data in a structured, commonly used, machine-readable format where applicable.

15.8 Right to Withdraw Consent

Where processing is based on consent, users may withdraw consent at any time.

15.9 Right Not to Be Subject to Solely Automated Decisions

Where applicable, users may object to solely automated decisions that produce legal or similarly significant effects.

Talent Pro does not intend to make final recruitment or hiring decisions solely through automated processing.

15.10 Right to Opt Out of Sale, Sharing, or Targeted Advertising

Where applicable under US state privacy laws or similar laws, users may have the right to opt out of:

1. Sale of personal data;
2. Sharing of personal data for cross-context behavioral advertising;
3. Targeted advertising;
4. Certain profiling activities.

Walumo does not sell personal data for money.

15.11 Right to Complain

Users may have the right to lodge a complaint with a data protection authority, privacy regulator, consumer protection authority, or other competent regulator in their jurisdiction.

16. How to Exercise Rights

Users may exercise their rights by contacting Walumo.

Walumo — Data Protection Contact

Email: infowalumo@walumoafrica.com

Where Walumo has appointed a formal Data Protection Officer or local representative, the contact details will be made available through the platform or relevant country notice.

Walumo may need to verify the user's identity before responding to a request.

Walumo aims to respond within 30 days unless a different period is required or allowed by applicable law.

17. Marketing Communications

Walumo may send marketing communications where:

1. The user has consented;
2. The communication is otherwise permitted by law;
3. The user has not opted out.

Marketing may include:

1. Job alerts;
2. Product updates;
3. Training opportunities;
4. Talent Pro announcements;
5. Career content;
6. Promotional offers;
7. Event invitations.

Users can opt out of marketing communications at any time by using the unsubscribe link or changing notification preferences.

Users may still receive transactional, service, security, legal, or account-related messages.

18. Cookies and Similar Technologies

Talent Pro uses cookies and similar technologies to:

1. Keep users logged in;
2. Secure sessions;
3. Remember preferences;
4. Support real-time messaging;
5. Measure platform performance;
6. Improve user experience;
7. Support AI sessions;
8. Process payments;
9. Deliver notifications;
10. Detect fraud or misuse.

More information is available in the Talent Pro Cookie and Tracking Technologies Policy.

Users can manage cookie preferences through:

Settings → Privacy → Cookie and Tracking Preferences

19. Mobile App Privacy

Where Talent Pro is available on iOS or Android, Walumo will disclose app data practices through the relevant app store privacy disclosures.

Talent Pro may request permissions for:

1. Notifications;
2. Camera access;
3. Photo or file uploads;
4. Microphone access where audio or interview features are enabled;
5. Biometric authentication where supported;
6. Device storage where necessary;
7. Location only where a feature clearly requires it.

Talent Pro will not access optional mobile permissions unless the user grants permission through the device operating system.

If Talent Pro uses tracking as defined by Apple or applicable law, Walumo will request the required permission before tracking.

Google Play Data Safety and Apple App Privacy declarations must match Talent Pro's actual data practices.

20. Children and Minors

Talent Pro is primarily intended for professional, recruitment, employment, training, and freelance use.

Talent Pro is not intended for children below the minimum legal age required in the relevant jurisdiction.

Where minors are permitted to use Talent Pro for internships, training, graduate programs, apprenticeships, or similar opportunities, Walumo will apply appropriate safeguards, which may include:

1. Parental or guardian consent where required;
2. Limited profiling;
3. Restricted marketing;
4. Limited data collection;
5. Stronger default privacy settings;
6. Additional review before AI processing;
7. Deletion controls.

21. Client, Employer, and Recruiter Responsibilities

Where an employer, recruitment agency, client, or organization uses Talent Pro, that organization is responsible for ensuring that its use of Talent Pro complies with applicable law.

This includes responsibility for:

1. Having a lawful basis for processing candidate data;
2. Providing appropriate notices to candidates where required;
3. Using candidate data fairly;
4. Avoiding discriminatory hiring practices;
5. Reviewing AI-assisted outputs responsibly;
6. Protecting recruiter and candidate data;
7. Deleting data when no longer needed;
8. Managing internal access rights;
9. Responding to user requests where it acts as controller;
10. Ensuring human oversight in recruitment decisions.

Walumo is not responsible for unlawful decisions made independently by recruiters, employers, or client organizations outside Talent Pro's control.

22. Data Accuracy

Users are responsible for ensuring that the information they provide is accurate, complete, and up to date.

Recruiters and employers are responsible for ensuring that notes, evaluations, statuses, and decisions entered into Talent Pro are accurate, fair, and lawful.

Users may update profile information through account settings or request correction through Walumo.

23. Public Profiles and Visibility

Talent Pro may allow users to control profile visibility.

Visibility settings may include:

1. Private profile;
2. Visible to recruiters after application;
3. Visible to selected recruiters;
4. Visible to partner organizations;
5. Public or community visibility, where enabled.

Users should review visibility settings carefully before making information available to others.

24. Third-Party Links and Integrations

Talent Pro may contain links to third-party websites, services, payment pages, login providers, employer pages, or external tools.

Walumo is not responsible for the privacy practices of third-party services that operate independently.

Users should review third-party privacy policies before using those services.

25. Data Breach and Incident Response

If Walumo becomes aware of a data security incident involving personal data, Walumo will investigate and take appropriate action.

Where required by law, Walumo will notify affected users, clients, regulators, or other competent authorities.

Walumo will maintain internal incident response procedures to manage security incidents.

26. Changes to This Privacy Policy

Walumo may update this Privacy Policy from time to time to reflect:

1. New Talent Pro features;
2. New AI capabilities;
3. New countries of operation;
4. New legal requirements;
5. New service providers;
6. New app store requirements;
7. Security improvements;
8. Changes to data processing practices.

If material changes are made, Walumo will provide appropriate notice through the platform, email, app notification, or another suitable channel.

The latest version of this Policy will be available through the Talent Pro platform.

27. Contact

For questions, privacy requests, complaints, or concerns about this Policy or Talent Pro's data practices, users may contact:

Walumo — Data Protection Contact

Email: infowalumoafrica.com

If a formal Data Protection Officer, EU representative, UK representative, or local representative is appointed, their details will be added to this Policy or the relevant country-specific notice.

Operational Privacy Compliance Checklist for Talent Pro

Before publishing this Privacy Policy or submitting Talent Pro to iOS or Android, Walumo must confirm the following:

Area	Requirement	Status
Data inventory	All data categories mapped	Pending
Data flows	Candidate, recruiter, employer, AI, payment, LMS, freelance, and community flows mapped	Pending
Lawful basis	Legal basis assigned to each processing purpose	Pending
AI governance	AI matching, scoring, embeddings, coaching, and recruiter support documented	Pending
Human review	Human review process for AI-assisted assessments documented	Pending
Third-party providers	All providers listed and reviewed	Pending
DPA/vendor contracts	Data processing terms in place with processors	Pending
International transfers	Transfer safeguards documented	Pending
Sensitive data	Sensitive-data handling process documented	Pending
Children/minors	Age and minor-use safeguards reviewed	Pending
Cookie policy	Cookie and tracking policy aligned with privacy policy	Pending

Consent	Consent system tested for marketing, cookies, AI, and optional permissions	Pending
Retention	Retention schedule approved	Pending
Deletion	Account deletion flow tested	Pending
Rights requests	Access, deletion, correction, portability, objection, and withdrawal process documented	Pending
Security	Encryption, access control, audit logs, backups, and incident process confirmed	Pending
Apple App Privacy	App Store privacy disclosures completed accurately	Pending
Apple ATT	ATT reviewed if tracking is used	Pending
Google Data Safety	Play Console Data Safety completed accurately	Pending
US state privacy	Do Not Sell/Share and opt-out obligations assessed	Pending
Kenya compliance	ODPC requirements assessed if processing Kenyan users	Pending
DRC compliance	Digital Code and local requirements assessed	Pending
South Africa compliance	POPIA requirements assessed if processing South African users	Pending
EU/UK compliance	GDPR/UK GDPR and AI Act implications assessed	Pending
Legal review	Qualified legal/privacy review completed	Pending
Final approval	Product, engineering, legal/data protection approval completed	Pending