OPTRACTION PRIVACY POLICY

Effective Date: 9 June 2026
Last Updated: 16 June 2026

1. Introduction

Welcome to Optraction, a project-first workspace where work, conversations and payments are brought together.

Optraction is a productivity, project-management and business-operations platform owned and operated by **Concept Colony Limited**, a company registered in the Federal Republic of Nigeria with registration number **9087914**.

This Privacy Policy explains how Concept Colony Limited collects, receives, uses, stores, shares, protects, transfers and otherwise processes personal data when individuals:

- Visit the Optraction website;
- Create or use an Optraction account;
- Create, manage or join a workspace;
- Participate in a project;
- Use project chats, task boards or time-tracking tools;
- Create, receive or pay invoices;
- Create or complete forms;
- Contact Optraction;
- Receive invitations or other communications;
- Participate in beta testing, product research or surveys;
- Connect an authorised third-party integration;
- Use any other Optraction service that refers to this Policy.

This Policy also explains the rights available to individuals and the procedures for exercising those rights.

This Privacy Policy is a transparency notice. It does not constitute blanket consent for every form of personal-data processing. Where consent is required for a specific processing activity, Optraction will request it separately and provide a reasonable method for withdrawing it.

---

2. Who We Are

Optraction is owned and operated by:

Legal entity: Concept Colony Limited
Company registration number: 9087914
Product: Optraction

General contact: contact@optraction.com
Privacy and Data Protection Officer contact: privacy@optraction.com

Concept Colony Limited is responsible for the processing of personal data in circumstances where it determines the purposes and methods of that processing.

---

3. Scope of This Policy

This Privacy Policy applies to personal data processed through:

- The Optraction public website;
- The Optraction web application;
- Any Optraction mobile application introduced in the future;
- User accounts and profiles;
- Personal and business workspaces;
- Workspace administration tools;
- Project dashboards;
- Project chats;
- Task boards;
- Time-tracking tools;
- Form-building and form-submission tools;
- Invoice and payment pages;
- Client and Guest portals;
- Subscription and billing services;
- Customer-support communications;
- Beta and early-access programmes;
- Authorised integrations;
- Any other Optraction-controlled service that refers to this Policy.

This Policy does not automatically govern websites, applications or services independently operated by third parties.

When users interact directly with an external service, that provider's own privacy policy and terms may apply.

---

4. Definitions

For the purposes of this Privacy Policy:

4.1 Personal Data

"Personal Data" means any information relating to an identified or identifiable natural person.

It may include:

- Names;
- Email addresses;
- Telephone numbers;
- Profile photographs;
- Account identifiers;
- IP addresses;
- Device identifiers;
- Professional information;
- Billing information;
- Messages;
- Location information;
- Payment records;
- Other information capable of identifying an individual directly or indirectly.

4.2 Processing

“Processing” means any operation performed on personal data, including:

- Collection;
- Recording;
- Organisation;
- Storage;
- Access;
- Use;
- Analysis;
- Transmission;
- Sharing;
- Updating;
- Restriction;
- Deletion;
- Destruction.

4.3 User Content

“User Content” means information, files, messages, documents and other materials created, uploaded, submitted, shared or stored through Optraction.

4.4 Workspace Customer

“Workspace Customer” means an individual, company, agency, partnership or organisation that creates, controls or pays for an Optraction workspace.

4.5 Workspace Owner

“Workspace Owner” means the individual authorised to manage a workspace, its subscription, members, permissions, projects and settings.

4.6 Team Member

“Team Member” means an internal collaborator invited to participate in a workspace or project.

4.7 Guest or Client

“Guest” or “Client” means an external participant invited to access a limited project, form, invoice, task board, client portal or related information.

4.8 Data Controller

A Data Controller determines why and how personal data will be processed.

4.9 Data Processor

A Data Processor processes personal data on behalf of and according to the instructions of a Data Controller.

---

5. Our Role as Data Controller and Data Processor

Concept Colony Limited may act as either a Data Controller or a Data Processor, depending on the nature of the information and the circumstances in which it is processed.

5.1 When We Act as a Data Controller

Concept Colony Limited generally acts as a Data Controller for personal data relating to:

- Account registration;
- User profiles;
- Subscription administration;
- Direct billing relationships;
- Platform security;
- Website enquiries;
- Customer support;
- Marketing preferences;
- Product research;
- Beta-programme administration;
- Legal compliance;
- Our direct relationship with users.

In these circumstances, Concept Colony Limited determines why and how the personal data is processed.

5.2 When We Act as a Data Processor

Concept Colony Limited may act as a Data Processor when a Workspace Customer uses Optraction to process personal data relating to:

- Clients;
- Employees;
- Team Members;
- Contractors;
- Guests;
- Form respondents;
- Invoice recipients;
- Project participants;
- Other individuals added to the workspace.

In these circumstances, the Workspace Customer may be the Data Controller, while Concept Colony Limited processes the information to provide the requested platform functions.

Where Optraction acts as a Data Processor, some privacy requests may need to be directed to the Workspace Customer that controls the relevant information.

We may assist the Workspace Customer with valid privacy requests where required by applicable law or a Data Processing Agreement.

5.3 Workspace Customer Responsibilities

Workspace Customers are responsible for:

- Having a lawful basis for uploading and using personal data;
- Providing appropriate privacy information to affected individuals;
- Obtaining consent where required;
- Limiting collection to information reasonably necessary;
- Assigning appropriate workspace permissions;
- Preventing unauthorised access;
- Responding to data-subject requests;
- Complying with applicable employment, privacy and commercial laws;
- Avoiding unnecessary collection of sensitive personal data.

A separate Data Processing Agreement may apply to certain business or enterprise customers.

---

6. Data Protection Officer

Concept Colony Limited will designate and maintain a suitably qualified **Data Protection Officer**, whether as an internal officer or through an external service arrangement.

The Data Protection Officer will be responsible for supporting and monitoring Optraction's compliance with applicable privacy and data-protection requirements.

The responsibilities of the Data Protection Officer may include:

- Advising management on data-protection obligations;
- Monitoring compliance with this Privacy Policy;
- Reviewing privacy notices and data-processing activities;
- Maintaining or supervising records of processing;
- Supporting privacy impact assessments;
- Reviewing data-security measures;
- Handling privacy complaints and rights requests;
- Supporting personal-data breach investigations;
- Advising on international data transfers;
- Reviewing service-provider and processor arrangements;
- Providing or coordinating privacy training;
- Communicating with the Nigeria Data Protection Commission where required.

The Data Protection Officer may be contacted at:

privacy@optraction.com

Until the appointment details of a named Data Protection Officer are published, this email address will remain the official contact point for privacy and data-protection matters.

---

7. Data-Protection Principles

Optraction aims to process personal data according to the following principles:

7.1 Lawfulness, Fairness and Transparency

Personal data will be processed using an appropriate lawful basis and in a manner that is reasonably understandable to affected individuals.

7.2 Purpose Limitation

Personal data will be collected for specific, explicit and legitimate purposes and will not be used incompatibly with those purposes.

7.3 Data Minimisation

We will seek to collect only the information reasonably necessary for the relevant purpose.

7.4 Accuracy

We will take reasonable steps to maintain accurate and complete personal data.

7.5 Storage Limitation

Personal data will not be retained for longer than necessary, subject to the three-year general retention period and any applicable legal exceptions described in this Policy.

7.6 Confidentiality, Integrity and Availability

We will maintain reasonable safeguards intended to protect information against unauthorised access, alteration, loss, disclosure or destruction.

7.7 Accountability

We will maintain appropriate records, policies and procedures to demonstrate compliance with applicable privacy obligations.

7.8 Duty of Care

We will consider the likely impact of our processing activities on affected individuals and apply safeguards proportionate to the risks involved.

---

8. Information We Collect

The information collected depends on how an individual interacts with Optraction.

8.1 Account and Profile Information

When a user creates or accesses an account, we may collect:

- Full name;
- Username;
- Email address;
- Telephone number;
- Profile photograph;
- Job title;
- Professional role;
- Company or organisation name;
- Country or region;
- Time zone;
- Language preference;
- Password or authentication information;
- Notification preferences;
- Workspace settings;
- Account status.

Passwords will not be stored in readable form. They should be protected through appropriate password-hashing and authentication controls.

8.2 Workspace and Membership Information

When a user creates or joins a workspace, we may process:

- Workspace name;
- Business information;
- User role;
- Membership status;
- Project assignments;
- Permissions;
- Invitation history;
- Workspace activity;
- Administrative actions;
- Seat allocation;
- Subscription status;
- Access records.

8.3 Project and Collaboration Information

When users create or participate in projects, we may process:

- Project names;
- Project descriptions;
- Client information;
- Deadlines;
- Milestones;
- Project status;
- Chat messages;
- Comments;
- Decisions;
- Approvals;
- Attachments;
- Member assignments;
- Activity history;
- Automated system updates.

Project information may be visible to authorised participants according to the permissions selected by the Workspace Owner.

8.4 Task and Workflow Information

We may process:

- Task titles;
- Task descriptions;
- Assigned users;
- Due dates;
- Priorities;

- Statuses;
- Comments;
- Attachments;
- Completion records;
- Editing history;
- Automated workflow activity.

8.5 Time-Tracking Information

Where time tracking is used, we may process:

- Timer start and stop times;
- Manually recorded entries;
- Duration;
- Task or project association;
- Entry descriptions;
- User responsible for the entry;
- Editing or approval history.

Workspace Customers are responsible for ensuring that their use of time tracking complies with applicable employment, contractor and privacy requirements.

8.6 Form Information

When users create or complete forms, we may process:

- Form titles;
- Questions;
- Responses;
- Names;
- Contact details;
- Project requirements;
- Service requests;
- Uploaded documents;
- Consent selections;
- Submission dates;
- Payment-related information;
- Form activity.

The user who creates a form is responsible for ensuring that the form has a lawful purpose and does not collect excessive or unlawful information.

8.7 Invoice and Payment Information

When invoicing and payment features are used, we may process:

- Invoice numbers;
- Client names;

- Client email addresses;
- Billing addresses;
- Service descriptions;
- Amounts;
- Currency;
- Due dates;
- Tax information;
- Payment status;
- Transaction references;
- Payment dates;
- Refund information;
- Chargeback information;
- Limited payer details;
- Paystack transaction responses.

8.8 Files and Attachments

Users may upload:

- Documents;
- Images;
- Videos;
- Audio files;
- Contracts;
- Briefs;
- Presentations;
- Spreadsheets;
- Design files;
- Reports;
- Other project materials.

Users must have the authority and an appropriate lawful basis to upload information relating to other individuals.

8.9 Communications with Optraction

We may collect information when users:

- Contact us by email;
- Request customer support;
- Submit a complaint;
- Request a refund;
- Report a security issue;
- Respond to a survey;
- Participate in product research;
- Submit feedback;
- Join a beta programme.

8.10 Technical and Security Information

Our systems and hosting infrastructure may automatically generate technical information such as:

- IP address;
- Browser type;
- Device type;
- Operating system;
- Login time;
- Session identifier;
- Authentication status;
- Failed login attempts;
- Approximate region derived from IP address;
- Server requests;
- Error information;
- Security events;
- Diagnostic information.

This information is used primarily to operate, secure and troubleshoot Optraction.

---

9. Information About Invitees and Non-Users

A person may receive an Optraction communication without previously creating an account.

A Workspace User may provide another person’s information to:

- Invite them to a project;
- Add them as a client;
- Send an invoice;
- Request completion of a form;
- Share a project update;
- Grant limited Guest access.

We may receive and process:

- The person’s name;
- Email address;
- Telephone number, where provided;
- The identity of the inviting user;
- The reason for the invitation;
- The relevant workspace, project, form or invoice;
- Delivery and response information.

We use this information to provide the requested invitation or service.

An invitee may contact **privacy@optraction.com** to raise an objection, request information or ask that appropriate action be taken regarding their personal data.

---

10. Sensitive Personal Data

Optraction is not intended to serve as a primary system for storing highly sensitive personal data.

Sensitive information may include information relating to:

- Health;
- Genetics;
- Biometrics used for identification;
- Religious or philosophical beliefs;
- Political opinions;
- Trade-union membership;
- Race or ethnic origin;
- Sexual life or orientation;
- Criminal allegations or convictions;
- Government identity documents;
- Financial-account credentials.

Users should not upload sensitive personal data unless:

- It is reasonably necessary;
- They have an appropriate lawful basis;
- Required privacy notices have been provided;
- Required consent has been obtained;
- Access is properly restricted;
- Appropriate security measures have been applied.

Optraction may restrict or remove sensitive information where its processing creates an unacceptable privacy, security or legal risk.

---

11. How We Use Personal Data

We may process personal data for the following purposes.

11.1 Providing Optraction

We use information to:

- Create and manage accounts;
- Authenticate users;
- Create and operate workspaces;

- Provide projects, tasks and chats;
- Provide time-tracking functions;
- Create and deliver invoices;
- Process forms;
- Send invitations;
- Provide Guest access;
- Maintain user preferences;
- Deliver requested platform features.

11.2 Subscription and Billing Administration

We may use information to:

- Activate paid plans;
- Calculate billable seats;
- Manage renewals;
- Process subscription payments;
- Send payment confirmations;
- Manage failed payments;
- Handle refund requests;
- Maintain transaction records;
- Meet tax and accounting obligations.

11.3 Payment Processing

We may use relevant information to:

- Initiate Paystack transactions;
- Confirm payments;
- Update invoice statuses;
- Reconcile transactions;
- Investigate failed or disputed payments;
- Prevent fraud;
- Respond to chargebacks;
- Maintain payment records.

11.4 Security and Fraud Prevention

We may process information to:

- Protect accounts;
- Detect suspicious activity;
- Prevent unauthorised access;
- Investigate fraud;
- Detect malware;
- Protect payment features;
- Enforce platform policies;
- Maintain audit records;

- Respond to incidents.

11.5 Customer Support

We may use information to:

- Respond to enquiries;
- Troubleshoot errors;
- Investigate account issues;
- Resolve billing problems;
- Support onboarding;
- Address complaints.

11.6 Product Development and Improvement

We may use appropriate information to:

- Identify technical errors;
- Test platform features;
- Improve usability;
- Measure system reliability;
- Understand common support problems;
- Improve accessibility;
- Develop new features.

Where reasonably possible, product analysis will use aggregated, de-identified or limited information.

11.7 Service Communications

We may send essential communications concerning:

- Account access;
- Security;
- Invitations;
- Project activity;
- Invoices;
- Form submissions;
- Subscription changes;
- Failed payments;
- Service interruptions;
- Policy updates;
- Legal notices;
- Support requests.

Users may not be able to opt out of essential service communications while maintaining an active account.

11.8 Marketing Communications

Where legally permitted, we may send:

- Product announcements;
- Newsletters;
- Educational resources;
- Event invitations;
- Beta invitations;
- Promotional offers.

Users may opt out of marketing messages without losing access to essential service communications.

11.9 Legal Compliance

We may process information to:

- Comply with laws;
- Respond to valid legal requests;
- Establish or defend claims;
- Enforce agreements;
- Protect intellectual property;
- Maintain required records;
- Respond to regulators;
- Investigate suspected violations.

---

12. Lawful Bases for Processing

Depending on the processing activity, we may rely on one or more of the following lawful bases.

12.1 Contract

Processing may be necessary to:

- Create an account;
- Provide platform features;
- Manage a subscription;
- Process an invoice;
- Provide support;
- Perform our agreement with a user.

12.2 Consent

We may rely on consent for:

- Optional marketing;

- Non-essential cookies;
- Certain sensitive-data processing;
- Optional research;
- Particular future integrations;
- Activities requiring express permission.

Consent may be withdrawn at any time, subject to applicable law.

12.3 Legal Obligation

We may process information to comply with:

- Tax laws;
- Accounting rules;
- Court orders;
- Regulatory duties;
- Data-protection obligations;
- Fraud-prevention requirements;
- Other applicable laws.

12.4 Legitimate Interests

We may process information where reasonably necessary to:

- Secure Optraction;
- Prevent fraud;
- Improve reliability;
- Provide business support;
- Protect legal rights;
- Understand platform performance;
- Maintain appropriate records.

Before relying on legitimate interests, we will consider the necessity of the processing, its likely impact and the safeguards available.

12.5 Vital Interests

In limited emergencies, information may be processed where necessary to protect a person's life or safety.

12.6 Other Lawful Grounds

We may rely on another lawful ground recognised under applicable data-protection law where appropriate.

---

13. Paystack Payment Processing

Optraction uses **Paystack** as its payment-processing provider.

When a payment is initiated, Paystack may collect or process information such as:

- Payer name;
- Email address;
- Telephone number;
- Payment-card information;
- Bank or payment-method information;
- IP address;
- Device information;
- Transaction amount;
- Currency;
- Transaction reference;
- Fraud and risk information.

Payment-card details may be entered directly into Paystack's payment environment.

Optraction may receive limited payment information, including:

- Transaction reference;
- Transaction status;
- Amount;
- Currency;
- Date and time;
- Payer name;
- Payer email;
- Masked payment-method information;
- Refund or chargeback status.

Optraction does not intend to store complete payment-card numbers or card security codes.

Paystack may process certain information independently under its own privacy policy, legal obligations and payment-security requirements.

Users who make or receive payments through Optraction may also be subject to Paystack's applicable terms and privacy practices.

---

14. Hosting and Cloud Infrastructure

Optraction uses third-party cloud hosting and infrastructure services to operate the website, application, databases, files, backups and related systems.

The hosting provider may process:

- Account information;
- Workspace data;
- Project data;

- Uploaded files;
- Technical records;
- Security logs;
- Database records;
- Backup copies.

The provider may act as a Data Processor on behalf of Concept Colony Limited.

We will seek to ensure that hosting and infrastructure providers are subject to appropriate:

- Confidentiality obligations;
- Data-processing terms;
- Security requirements;
- Access limitations;
- Incident-notification obligations;
- International-transfer safeguards where applicable.

The name and processing location of the confirmed production hosting provider should be included in Optraction's service-provider or subprocessor register.

---

15. Cookies and Tracking Technologies

At the date of this Policy:

- Optraction does not use third-party advertising cookies;
- Optraction does not use behavioural advertising tools;
- Optraction does not use remarketing pixels;
- Optraction does not use social-media tracking pixels;
- Optraction does not use cross-site behavioural tracking;
- Optraction does not use third-party analytics for advertising profiling.

Optraction may use strictly necessary first-party cookies and browser-storage technologies to:

- Maintain secure login sessions;
- Authenticate accounts;
- Protect forms;
- Remember essential preferences;
- Support basic platform functionality;
- Remember cookie choices.

If non-essential analytics, advertising or tracking technologies are introduced:

- This Privacy Policy will be updated;
- The Cookie Policy will be updated;
- The provider and purpose will be disclosed;
- Retention periods will be explained;
- Consent will be requested where required;

- Users will be provided with appropriate controls.

---

16. How We Share Personal Data

Optraction does not sell personal data.

We may share personal data in the following circumstances.

16.1 Workspace Participants

Information may be shared with authorised:

- Workspace Owners;
- Team Members;
- Guests;
- Clients;
- Project participants.

Visibility depends on the permissions and access settings selected by the Workspace Owner.

16.2 Paystack

Information necessary for payments, transaction confirmation, refunds, fraud prevention and reconciliation may be shared with Paystack.

16.3 Hosting and Infrastructure Providers

Information may be processed by hosting, storage, backup and infrastructure providers that support Optraction.

16.4 Other Service Providers

As Optraction grows, we may engage providers for:

- Email delivery;
- Authentication;
- Customer support;
- Security monitoring;
- File storage;
- Error monitoring;
- Communications;
- AI-assisted functions.

A provider will receive only information reasonably necessary for the service it supplies.

16.5 Integrations Requested by Users

Where a user connects an external service, information may be shared as necessary to operate the requested integration.

16.6 Professional Advisers

Information may be shared with lawyers, accountants, auditors, insurers or compliance advisers for legitimate professional purposes.

16.7 Legal Authorities

We may disclose information where reasonably necessary to:

- Comply with law;
- Respond to a valid court order;
- Respond to a regulatory request;
- Investigate fraud or crime;
- Protect users;
- Prevent serious harm;
- Establish or defend legal rights.

16.8 Business Transactions

Information may be transferred or disclosed in connection with a merger, acquisition, investment, restructuring, financing or sale of the Optraction business, subject to appropriate confidentiality safeguards.

---

17. International Data Transfers

Optraction’s hosting, payment or service providers may process information outside Nigeria.

Where personal data is transferred internationally, we will seek to establish an appropriate lawful transfer basis and reasonable safeguards.

Depending on the circumstances, these may include:

- Adequacy determinations;
- Approved contractual safeguards;
- Standard contractual clauses;
- Recognised transfer agreements;
- Binding corporate rules;
- Legally recognised exceptions;
- Explicit consent where appropriate;
- Additional technical and organisational safeguards.

We may assess:

- The destination country;
- The nature and sensitivity of the information;
- The recipient's security measures;
- Applicable privacy protections;
- Risks to affected individuals;
- Available contractual and technical protections.

---

18. Data Retention

Optraction applies a general retention period of **three years**.

Unless a shorter or longer period is required by law or justified by a specific purpose, personal data may be retained for up to three years after:

- The account is closed;
- The workspace is deleted;
- The user's relationship with Optraction ends;
- The relevant project is completed;
- The relevant transaction or interaction occurs;
- The information is last actively required.

18.1 Account and Profile Information

Account and profile information may be retained for up to three years after account closure for:

- Security;
- Fraud prevention;
- Account recovery;
- Dispute handling;
- Legal compliance.

18.2 Workspace and Project Information

Workspace content, including projects, tasks, messages, forms, time records and files, may be retained for up to three years after the workspace is closed or deleted.

A valid deletion request may result in earlier deletion where:

- No legal obligation requires retention;
- No payment dispute is active;
- No legal claim requires preservation;
- No other lawful basis supports continued retention.

18.3 Invoice and Payment Information

Invoice and transaction information may be retained for three years or for a longer period where required by:

- Tax law;
- Accounting rules;
- Payment-provider requirements;
- Fraud prevention;
- Chargeback procedures;
- Court proceedings;
- Other legal obligations.

Paystack may retain payment information according to its own legal and operational requirements.

18.4 Form Submissions

Form submissions may be retained for up to three years after submission or until the Workspace Customer deletes them, subject to applicable legal exceptions.

18.5 Invitations

Expired or unused invitations may be retained for up to three years for:

- Delivery verification;
- Security;
- Fraud prevention;
- Dispute handling;
- Suppression of unwanted messages.

18.6 Support and Privacy Communications

Support, complaint and privacy-request records may be retained for up to three years after the matter is closed.

18.7 Security Logs

Security and access logs may be retained for up to three years where proportionate to:

- Cybersecurity risks;
- Fraud investigations;
- Account protection;
- Legal requirements.

18.8 Backups

Deleted information may remain temporarily in secure or restricted backups until the backup cycle is completed.

Backup information will not ordinarily be restored to active use except for:

- Disaster recovery;
- Security investigation;
- Legal compliance;
- System restoration.

When information is no longer required, we will take reasonable steps to delete, anonymise, aggregate or securely destroy it.

---

19. Security Measures

Optraction maintains a baseline information-security programme intended to protect the confidentiality, integrity and availability of personal data.

The measures applied or required for the production platform include the following.

19.1 Encryption in Transit

Communications between users and Optraction should be protected using HTTPS and current Transport Layer Security protocols.

19.2 Encryption at Rest

Personal data, databases, files and backups should be encrypted at rest where supported and appropriate to the risk involved.

19.3 Password Security

Passwords should be:

- Hashed using an appropriate password-hashing algorithm;
- Protected with unique salts;
- Never stored in readable plain text;
- Subject to reasonable password-strength requirements.

19.4 Role-Based Access Control

Access to personal data should be based on:

- Workspace roles;
- Project membership;
- Job responsibilities;
- Least-privilege principles;
- Need-to-know access.

19.5 Administrative Account Protection

Administrative and privileged accounts should use:

- Strong authentication;
- Multi-factor authentication where available;
- Restricted permissions;
- Periodic access reviews;
- Separate credentials from ordinary user accounts.

19.6 Session Security

Optraction should apply:

- Secure session tokens;
- Session-expiration controls;
- Protection against session theft;
- Logout and revocation mechanisms;
- Controls against unauthorised requests.

19.7 Secure Cloud Configuration

Hosting infrastructure should be configured to:

- Restrict unnecessary public access;
- Protect database and storage services;
- Apply network and firewall controls;
- Separate production and development environments where appropriate;
- Limit administrative interfaces.

19.8 Secure Software Development

Development practices should include:

- Code review;
- Dependency management;
- Secure configuration;
- Testing before deployment;
- Protection of secrets and credentials;
- Correction of known vulnerabilities;
- Separation of testing and production information where appropriate.

19.9 Vulnerability and Patch Management

Systems, libraries and dependencies should be:

- Monitored for known security issues;
- Updated within reasonable periods;

- Patched according to risk;
- Reviewed following significant incidents.

19.10 Logging and Monitoring

Optraction may maintain logs for:

- Login activity;
- Administrative access;
- Permission changes;
- Failed authentication;
- Security events;
- Application errors;
- Relevant payment events.

Access to logs should be restricted and logs should not contain unnecessary sensitive information.

19.11 Backups and Recovery

Optraction should maintain:

- Secure backups;
- Restricted access to backups;
- Recovery procedures;
- Periodic backup testing;
- Backup-retention controls.

19.12 Staff and Contractor Controls

Persons with access to personal data should be subject to:

- Confidentiality obligations;
- Access limitations;
- Privacy and security awareness;
- Appropriate onboarding and offboarding procedures;
- Removal of access when no longer required.

19.13 Service-Provider Reviews

Before engaging material service providers, Optraction should consider:

- Security practices;
- Privacy terms;
- Processing locations;
- Breach-notification procedures;
- Subprocessor arrangements;
- Contractual safeguards.

19.14 Incident Response

Optraction should maintain procedures for:

- Identifying incidents;
- Containing risks;
- Preserving evidence;
- Assessing affected information;
- Notifying management;
- Notifying regulators or individuals where required;
- Correcting identified weaknesses.

19.15 Data Minimisation and Deletion

Systems should be configured, where reasonably possible, to:

- Collect only necessary information;
- Restrict unnecessary access;
- Delete expired information;
- Prevent indefinite retention;
- Reduce unnecessary copies.

These security measures will be reviewed periodically and adjusted according to the nature of the information, available technology and identified risks.

No electronic platform can guarantee absolute security.

---

20. Personal-Data Breaches

A personal-data breach may include accidental or unlawful:

- Destruction;
- Loss;
- Alteration;
- Disclosure;
- Access;
- Unavailability of personal data.

Where Optraction becomes aware of a suspected breach, we will take reasonable steps to:

1. Investigate the incident;
2. Contain the risk;
3. Identify affected systems and individuals;
4. Assess the likely consequences;
5. Preserve relevant records;
6. Take corrective action;

7. Inform affected Workspace Customers where appropriate;
8. Notify the Nigeria Data Protection Commission within the legally required period where applicable;
9. Notify affected individuals where legally required;
10. Review measures intended to prevent recurrence.

Where applicable, a qualifying personal-data breach will be reported to the Nigeria Data Protection Commission within **72 hours of becoming aware of it**.

Users should report suspected privacy or security incidents immediately to:

privacy@optraction.com

---

21. Workspace Owner and Administrator Access

Workspace Owners and authorised administrators may be able to:

- Access workspace information;
- View member profiles;
- Review projects;
- Review activity;
- Manage permissions;
- Export records;
- Remove members;
- Delete projects;
- Control integrations;
- Manage subscriptions.

Users should understand that information created within a business workspace may be controlled by the relevant Workspace Customer.

Where a user leaves an organisation:

- Their access may be removed;
- The organisation may retain business records;
- Project messages may remain in the workspace;
- Work records may remain available to authorised administrators;
- The user may lose access to workspace content.

---

22. User Rights

Depending on applicable law and the circumstances, individuals may have the following rights.

22.1 Right to Be Informed

The right to receive information about how personal data is processed.

22.2 Right of Access

The right to request confirmation of processing and access to relevant personal data.

22.3 Right to Correction

The right to request correction of inaccurate or incomplete information.

22.4 Right to Deletion

The right to request deletion where an applicable legal basis exists.

Deletion may be limited where retention is necessary for:

- Legal obligations;
- Tax or accounting requirements;
- Fraud prevention;
- Payment disputes;
- Security;
- Legal claims;
- Another person’s lawful rights.

22.5 Right to Restriction

The right to request temporary restriction of certain processing activities.

22.6 Right to Object

The right to object to certain processing based on legitimate interests or direct marketing.

22.7 Right to Withdraw Consent

Where processing is based on consent, the individual may withdraw that consent.

Withdrawal applies to future processing and does not invalidate earlier lawful processing.

22.8 Right to Data Portability

Where applicable, the right to receive certain information in a structured and commonly used format.

22.9 Rights Concerning Automated Decisions

Where applicable, individuals may request:

- Information about significant automated processing;
- Human review;
- An opportunity to provide their position;
- Reconsideration of a decision;
- An opportunity to challenge a result.

22.10 Right to Complain

Individuals may complain to Optraction or to the Nigeria Data Protection Commission.

---

23. Exercising Privacy Rights

Requests should be submitted to:

privacy@optraction.com

A request should include, where possible:

- The individual's name;
- The relevant account email;
- The workspace involved;
- The right being exercised;
- A description of the request;
- Information needed to locate the relevant records.

We may request reasonable identity verification before disclosing, changing or deleting information.

Where Optraction acts as a Data Processor, we may:

- Refer the request to the relevant Workspace Customer;
- Notify the Workspace Customer;
- Assist the Workspace Customer;
- Explain why that customer controls the relevant information.

We will respond within the period required by applicable law.

---

24. Marketing Preferences

Users may opt out of marketing communications by:

- Using the unsubscribe option contained in the communication; or
- Contacting privacy@optraction.com.

Opting out of marketing will not stop essential communications relating to:

- Security;
- Account administration;
- Billing;
- Invitations;
- Invoice delivery;
- Project activity;
- Legal notices;
- Service operation.

Optraction does not sell personal data to advertisers.

---

25. Automated Processing and Artificial Intelligence

Optraction may introduce automation or AI-assisted features for:

- Project summaries;
- Task suggestions;
- Workflow recommendations;
- Draft messages;
- Reporting;
- Categorisation;
- Security monitoring;
- Fraud prevention;
- Productivity insights.

At the date of this Policy:

- Optraction does not make decisions producing legal or similarly significant effects solely through automated processing;
- Optraction does not use private workspace content to train general-purpose AI models;
- Optraction does not use AI to determine access to employment, credit, insurance or public benefits.

Where AI functions are introduced:

- Their purpose will be explained;
- Relevant information use will be disclosed;
- Appropriate controls will be provided;

- Significant outputs should remain subject to human review.

Private User Content will not be used to train a general-purpose AI model without:

- Clear notice;
- An appropriate lawful basis;
- Required consent;
- Reasonable safeguards.

---

26. Children and Minors

Optraction is primarily intended for businesses, agencies, freelancers, professionals, clients and service teams.

Individuals under 18 should not independently:

- Create or control a paid workspace;
- Purchase a subscription;
- Enter into a binding commercial agreement through Optraction.

A minor may participate only where:

- Their participation is lawful;
- Appropriate parental, guardian, school, employer or organisational authorisation exists;
- The Workspace Customer is authorised to provide access;
- Reasonable safeguards are applied.

We do not knowingly target children with behavioural advertising or profiling.

---

27. Third-Party Services

Optraction may integrate with or link to external services.

Third-party services may process personal data under their own:

- Privacy policies;
- Terms;
- Security practices;
- Retention rules;
- Legal obligations.

Optraction does not control the independent processing activities of external providers.

Users should review the privacy information of third-party services before connecting or using them.

---

28. Privacy by Design and Impact Assessments

Optraction will seek to consider privacy and data protection when designing:

- New features;
- Payment tools;
- Integrations;
- AI systems;
- Public-sharing tools;
- Analytics services;
- High-risk processing activities.

Where required or appropriate, Optraction may conduct a Data Privacy Impact Assessment before introducing processing likely to create a significant risk to individuals.

Such assessments may consider:

- Necessity;
- Proportionality;
- Data minimisation;
- Access controls;
- Retention;
- Security;
- International transfers;
- Risks to vulnerable individuals;
- Available safeguards.

---

29. Changes to This Privacy Policy

We may update this Privacy Policy to reflect:

- Platform changes;
- New features;
- New integrations;
- Changes to Paystack or another provider;
- A confirmed hosting provider;
- New AI functionality;
- Legal developments;
- Security improvements;
- Changes to processing purposes.

The revised version will display an updated date.

Where a change materially affects how personal data is processed, we may notify users through:

- Email;

- In-app messages;
- Dashboard notices;
- Website notices;
- Another appropriate method.

Where consent is required for a new activity, Optraction will request that consent rather than treating continued use as automatic consent.

---

30. Complaints

Privacy complaints may be submitted to:

privacy@optraction.com

A complaint should include:

- The individual's name;
- Relevant account email;
- Relevant workspace;
- Description of the concern;
- Supporting information;
- The requested resolution.

We will investigate and respond within applicable legal timeframes.

Individuals may also lodge a complaint with the **Nigeria Data Protection Commission**.

Nothing in this Policy limits a person's right to seek an available legal remedy.

---

31. Governing Privacy Framework

This Privacy Policy is intended to be interpreted consistently with:

- The Constitution of the Federal Republic of Nigeria;
- The Nigeria Data Protection Act 2023;
- Applicable directives issued by the Nigeria Data Protection Commission;
- Applicable cybersecurity and consumer-protection requirements.

Nothing in this Policy limits mandatory privacy rights available under laws that apply to an individual.

---

32. Contact Information

For privacy questions, rights requests, security concerns or complaints, contact:

Concept Colony Limited
Registration Number: 9087914
Product: Optraction

Privacy and DPO contact: privacy@optraction.com
General contact: contact@optraction.com
Registered business address: [Insert registered business address]

Suggested email subjects include:

- Privacy Rights Request
- Data Access Request
- Data Correction Request
- Data Deletion Request
- Security Incident
- Privacy Complaint
- Data Processing Enquiry