

Privacy Policy

Global policy for the Contlant website and ScopeSpace product suite

Effective date	21 September 2026
Organisation	Contlant Limited
Primary contact	privacy@contlant.com
Service reach	International
Version	V1
Company number	PVT-DLUP8X5A
Registered address	Muthithi Road, Westlands, Nairobi, Kenya
Contact	privacy@contlant.com +254 780 074 521

Contlant Limited is established in Kenya and provides ScopeSpace to customers and users in multiple countries. This policy explains our global approach to personal data and the additional protections that may apply under the law of a user's location.

1 About this policy

Contlant Limited ("Contlant", "we", "us" or "our") is a technology company incorporated in Kenya. We provide the Contlant website and the ScopeSpace business software platform, including ScopePayroll, ScopeBooks, ScopeTax, ScopeStock and ScopeAppointments. ScopeSpace is offered internationally and may be accessed from countries where its use is permitted. Kenya is our place of incorporation, but this policy is written for a global user base and is not limited to the Kenyan market.

This policy describes the personal data we collect, the reasons we use it, the parties with whom we share it, how long we keep it, the safeguards we apply and the rights available to individuals. It applies to website visitors, prospective customers, customers, authorised users, employees and other workers whose records are placed in ScopeSpace, appointment clients, suppliers and business contacts in any country. It also applies to users who connect Google Calendar, Microsoft Outlook or Microsoft 365 Calendar, or iCloud Calendar to ScopeAppointments.

The policy does not replace a customer's own privacy notice to its employees, clients, suppliers or other individuals. Customers remain responsible for telling those individuals how the customer uses their information and for establishing a lawful basis for placing that information in ScopeSpace.

2 Our role as controller and processor

Our legal role depends on why personal data is processed and who decides the purpose and means of that processing.

1. **Contlant as data controller.** We act as controller for information used to operate our website, manage enquiries, administer customer and user accounts, process subscriptions and billing, provide support, protect the platform, improve service reliability, communicate about our services and meet our own legal obligations.
2. **Contlant as data processor.** A customer is normally the controller of employee, payroll, tax, accounting, supplier, inventory, appointment and other operational records that the customer or its authorised users place in ScopeSpace. We process that information on the customer's documented instructions to provide and secure the service.
3. **Independent third parties.** Payment providers, calendar providers and other third parties may act as independent controllers for information they process under their own terms. Their privacy notices apply to that separate processing.

If you are an employee, appointment client, supplier or other individual whose information was placed in ScopeSpace by a customer, contact that customer first about your rights. We will assist the customer as required by our agreement and applicable law.

3 Personal data we collect

Context	Personal data that may be processed
Website and enquiries	Name, organisation, work email, phone number, product interest, team size, message, consent record, referral information, IP address, browser and device data.

Context	Personal data that may be processed
Public payroll calculator	Salary and deduction figures, tax-residency and employment selections, calculation date and technical request data. A personalised PDF may also include the name and email entered by the user.
Accounts and identity	Name, email, organisation, role, permissions, authentication events, Google sign-in identifier where selected, session and security records.
Subscriptions and billing	Plan, billing contact, transaction and subscription references, invoice information, payment status and limited payment metadata. Full card or mobile-money credentials are handled by the payment provider.
ScopePayroll	Employee identity and contact details, employment terms, salary and benefits, deductions, payroll results, tax and social-security identifiers, bank and payment details, payslips, approvals and audit history.
ScopeBooks	Customer and supplier contacts, invoices, expenses, ledger records, bank and payment references, reconciliation information, supporting documents and audit history.
ScopeTax	Taxpayer identifiers, tax profiles, calculations, obligations, filing and payment records, supporting evidence, correspondence and review history.
ScopeStock	Users responsible for stock activities, supplier and customer contacts, item, location and movement records, approvals, notes and audit history.
ScopeAppointments	Names, contact details, organisation, booking reason, appointment time, assigned host, location, meeting link, notes, attendance status, reminders and consent record.
Calendar integrations	Provider account identifier, calendar lists, event titles, times, attendees, locations, meeting links, availability data, encrypted access tokens or an encrypted iCloud app-specific password, and synchronisation logs.
Support and security	Support requests, correspondence, diagnostic details, IP address, user agent, sign-in attempts, access logs, administrative actions, security events and incident records.

4 How we collect personal data

We collect personal data from the following sources:

- directly from you when you browse the website, use a calculator, submit a form, create or use an account, communicate with us, connect an integration or request support;
- from the organisation that employs, engages or serves you when it enters or imports records into ScopeSpace;
- from authorised users who create bookings, payroll records, accounting entries, supplier records, tax records or other operational information;
- from service providers and integrations, including Paystack, Google, Microsoft and Apple, when you or a customer choose to use the relevant service;
- automatically through server logs, security tools, strictly necessary cookies and local storage; and
- from public records or lawful business sources where this is necessary and permitted by law.

5 How we use personal data

We use personal data only for specified business and service purposes, including to:

- provide, configure and support the website, ScopeSpace and subscribed products;
- authenticate users, maintain sessions, enforce permissions and isolate customer workspaces;
- calculate payroll and tax results, prepare documents, maintain accounting and inventory records, coordinate appointments and synchronise connected calendars;
- process orders, subscriptions, invoices and payment confirmations;
- respond to enquiries, quotations, onboarding requests and support tickets;
- send service messages, security notices, booking communications and other transactional communications;
- detect, investigate and prevent fraud, abuse, unauthorised access and service disruption;
- monitor reliability, diagnose errors, maintain audit records and improve product performance;
- comply with law, lawful requests, accounting and tax obligations, and establish or defend legal claims; and
- send marketing communications where permitted and where any required consent has been obtained.

6 Lawful bases for processing

Where we act as controller, we rely on one or more lawful bases recognised by applicable data-protection law. These include the Kenya Data Protection Act, 2019 and, where their territorial requirements are met, the European Union General Data Protection Regulation, the United Kingdom General Data Protection Regulation and comparable laws in other jurisdictions. The applicable basis depends on the activity and the individual's location.

Lawful basis	Typical use
Contract or steps before contract	Providing accounts and subscribed services, responding to requested quotations, processing payments and delivering support.
Legal obligation	Maintaining required business and accounting records, responding to lawful authority requests and meeting data-protection obligations.
Legitimate interests	Securing and improving the service, preventing fraud, maintaining audit trails, managing business relationships and communicating with business users where those interests do not override individual rights.
Consent	Optional analytics, marketing, selected integrations and other processing for which the law or the circumstances require a freely given choice. Consent may be withdrawn at any time without affecting earlier lawful processing.
Vital interests or public interest	Exceptional circumstances where processing is necessary to protect a person or carry out a legally recognised public-interest task.

Where we act as processor, the customer determines the lawful basis for its processing. In employment and payroll contexts this may include the employment relationship, statutory payroll and tax obligations, and other lawful grounds available to the customer.

7 Sensitive personal data

ScopeSpace may contain information that is sensitive under Kenyan law, including financial information, property details, family information, health-related deductions or benefits, biometric or identification information where a customer lawfully chooses to record it, and other data requiring additional protection. We process sensitive personal data only where a lawful condition applies and only to the extent necessary for the relevant service. Customers must avoid uploading sensitive information that is not required for a defined business purpose.

8 Public calculator

When the ScopeSpace calculation service is available, the public ScopePayroll calculator sends the calculation fields entered by the user securely to our service only to return the estimate. We do not intentionally retain those calculation inputs after the response, and salary amounts are not sent to website analytics. If the service cannot be reached, the matching calculation may run in the browser. Estimates deliberately saved in the browser remain on that device unless the user chooses to move them into ScopeSpace or generate a personalised document.

9 Cookies and local storage

We use cookies and similar technologies for distinct purposes. Strictly necessary cookies support authentication, secure sessions, fraud prevention and requested features. Local storage may remember an authenticated optional preference, calculator estimate or interface preference. Contlant does not activate optional analytics technologies on pre-login pages under V1. We do not use payroll, tax, accounting, calendar or appointment content for third-party behavioural advertising.

Browser settings can block or remove cookies and local storage. Blocking strictly necessary technologies may prevent sign-in, connected integrations or other protected features from working correctly.

10 Calendar integrations

ScopeAppointments can connect to Google Calendar, Microsoft Outlook or Microsoft 365 Calendar, and iCloud Calendar. The connection is optional and is initiated by an authorised user. We use approved permissions to list calendars, read availability and event information, detect conflicts, create or update events requested through ScopeAppointments and maintain a synchronised calendar view. ScopeSpace does not request mailbox access for this feature.

OAuth tokens and iCloud app-specific passwords are encrypted and used server-side. We do not ask for or store a primary Apple Account password. A user can disconnect a calendar at any time. Disconnection stops new synchronisation and removes or makes unusable the stored connection credentials, subject to limited backup, audit and legal-retention requirements.

Our use and transfer of information received from Google APIs is intended to comply with the Google API Services User Data Policy, including its Limited Use requirements. We do not sell calendar data, use it for advertising or use it to train general-purpose artificial-intelligence or machine-learning models.

11 Sharing personal data

We may share personal data with the following recipients only where necessary for the stated purposes:

- customer administrators and authorised users, according to the customer's roles and permissions;
- hosting, infrastructure, database, backup, email and technical support providers that help us operate the service;
- Paystack and related payment channels for checkout, subscription status, payment confirmation and reconciliation;
- Google, Microsoft or Apple when an authorised user connects the relevant identity or calendar service;
- professional advisers, auditors and insurers under duties of confidentiality;
- courts, regulators, law-enforcement agencies and public authorities where disclosure is required or permitted by law;
- a purchaser, investor or successor involved in a proposed or completed business transaction, subject to confidentiality and lawful safeguards; and
- another person where you direct us to share information or give valid consent.

We do not sell personal data. We require service providers acting for us to protect personal data, use it only for authorised purposes and apply appropriate security and confidentiality measures.

12 International transfers

ScopeSpace is an international service. Contlant operates from Kenya, and our hosting, payment, calendar, email and other service providers may process information in Kenya or other countries. Customer administrators and authorised users may also access their organisation's information from different countries. As a result, personal data may be transferred to, stored in or accessed from a country whose privacy laws differ from those of the country where the individual is located.

We apply the transfer requirements that govern the relevant data. Transfers from Kenya will use safeguards permitted by Kenyan law. Where the EU GDPR applies, transfers outside the European Economic Area will rely on an adequacy decision, approved standard contractual clauses or another lawful mechanism, together with supplementary measures where required. Where the UK GDPR applies, we will use UK adequacy regulations, the International Data Transfer Agreement, the UK Addendum to approved contractual clauses or another permitted safeguard or exception.

We assess service providers and transfer arrangements in light of the information involved, the destination, available contractual commitments and technical safeguards. Customers may contact us for available information about the countries, providers and transfer safeguards relevant to their service configuration.

13 Retention and deletion

We keep personal data only for as long as reasonably necessary for the purpose for which it was collected, the customer's documented instructions, the applicable customer agreement and legal requirements. We consider the sensitivity and volume of the data, security and dispute risks, statutory recordkeeping duties, contractual commitments and whether the purpose can be achieved using anonymised information.

Record type	Retention approach
-------------	--------------------

Record type	Retention approach
Anonymous calculator inputs	Not intentionally retained after the calculation response, apart from transient security and service logs that do not intentionally record salary figures.
Enquiries and prospects	Kept while we respond and for a reasonable follow-up and accountability period, then deleted or anonymised unless a business relationship begins or law requires longer retention.
Account, contract and billing records	Kept during the customer relationship and afterward for applicable accounting, tax, fraud-prevention, audit, dispute and legal requirements.
Customer-controlled workspace data	Kept for the active service period and then returned, exported, deleted or anonymised under the customer agreement, the customer's lawful instructions and mandatory recordkeeping duties.
Calendar credentials	Kept while the integration remains connected. On disconnection they are deleted or made unusable, subject to limited backups, security records and legal requirements.
Security and audit logs	Kept for a period proportionate to investigation, fraud prevention, access accountability, service integrity and legal requirements.
Backups	Protected and removed through the applicable backup-rotation cycle. Information may remain inaccessible in a backup until that copy expires or is securely overwritten.

Deletion may be delayed where information must be preserved for a legal obligation, active dispute, security investigation or lawful authority request. Where complete deletion is not required or technically immediate, we may restrict access, isolate the record or irreversibly anonymise it.

14 Security

We use technical and organisational measures designed for the nature and risk of the information processed. These include secure transport, protected session cookies, role-based access, server-side authorisation, customer and tenant separation, audit records, rate limiting, restricted administrative access, encrypted calendar credentials and encryption of selected restricted financial fields. We review safeguards as the service and risks change.

No internet service can guarantee absolute security. Customers must protect credentials, assign the least access necessary, review user access, keep source information accurate and notify us promptly of suspected misuse or compromise.

If a personal-data breach creates a real risk of harm, we will notify the Office of the Data Protection Commissioner without delay and within the period required by law, and will communicate with affected individuals where required. When we act as processor, we will notify the relevant customer without delay and within the period required by law.

15 Automated processing and assisted features

ScopeSpace uses deterministic rules and calculations to produce payroll, tax, accounting, inventory and scheduling outputs. Important outputs are intended for review by authorised users. The service is not

designed to make employment, credit or other decisions that produce legal or similarly significant effects solely by automated processing.

If an optional assisted or artificial-intelligence feature is introduced, we will describe the information it uses, the provider and transfer implications where relevant, the controls available to the customer and whether human approval is required. Such a feature will not use customer content to train a general-purpose model unless that use has been expressly disclosed and lawfully agreed.

16 Direct marketing

We may send information about Contlant products or services where the recipient has consented or another lawful basis permits the communication. Marketing messages will identify the sender and provide a practical way to opt out. Withdrawing from marketing does not stop essential service, security, billing or transactional messages. We do not disclose payroll, tax, accounting, appointment or calendar content to advertising partners.

17 Your data protection rights

Subject to the law that applies to you and any lawful limitations, you may have the right to:

- be informed about how your personal data is used;
- request access to personal data held about you;
- request correction of inaccurate or misleading personal data;
- request deletion or erasure where the legal conditions are met;
- object to processing, including direct marketing;
- request restriction of processing in appropriate circumstances;
- receive or transfer eligible personal data in a structured, commonly used and machine-readable format;
- withdraw consent at any time where processing depends on consent; and
- request reconsideration of a decision that has legal or similarly significant effects and was based solely on automated processing.

To exercise a right, email privacy@contlant.com and describe the information and request. We may need to verify identity and authority before acting. An authorised agent may submit a request where local law permits. We may ask for clarification where a request is broad or where another organisation controls the relevant record. We will respond within the period required by applicable law. Rights may be limited where retention or processing is required by law, necessary for legal claims, or subject to another lawful exception.

18 Additional rights by region

European Economic Area United Kingdom and Switzerland

Where the EU GDPR, UK GDPR or Swiss data-protection law applies, individuals may have rights of access, rectification, erasure, restriction, objection, portability, withdrawal of consent and protection from decisions based solely on automated processing. They may complain to the data-protection authority in the country where they live or work, or where the alleged infringement occurred. If applicable law requires Contlant to appoint a local representative, the representative's details will be published in this policy or an applicable regional notice.

United States

Residents of a US state with a comprehensive privacy law may, subject to that law and its thresholds or exceptions, request access to or confirmation of personal information, correction, deletion and portability. They may also have rights to opt out of a sale, sharing for cross-context behavioural advertising, targeted advertising or certain profiling; to limit specified uses of sensitive personal information; to use an authorised agent; to appeal a denied request; and to receive equal service when exercising privacy rights. Contlant does not sell personal data or share it for cross-context behavioural advertising.

Other countries and territories

Privacy laws in other countries may grant similar or additional rights. We will assess a request under the law applicable to the individual and the processing. Providing the same practical right to all users does not mean that every listed law applies to every activity.

19 Children

The public website and ScopeSpace are business services and are not directed to children. We do not knowingly invite a child to create an account. A customer must not place a child's personal data in ScopeSpace unless it has a lawful purpose, has provided the required notice, has obtained any required parental or guardian consent and has applied safeguards appropriate to the child's best interests.

20 Links and third party services

Our website and products may link to or integrate with third-party services. This policy does not control a third party's independent processing. Review that provider's privacy notice before supplying information or enabling an integration. Connecting or disconnecting a provider does not change information the provider independently holds under its own terms.

21 Changes to this policy

We may update this policy to reflect changes in law, our services, providers or processing practices. The published version will state its effective date. We will use an appropriate service channel to communicate material changes that significantly affect how personal data is used or the choices available to individuals.

22 Contact and complaints

For questions, complaints or requests concerning this policy or Contlant's handling of personal data, contact:

Contlant Limited

Nairobi, Kenya

Email: privacy@contlant.com

If your concern relates to information controlled by a ScopeSpace customer, you should ordinarily contact that customer first. You may complain to the data-protection or privacy regulator in your country or region where the law permits. Because Contlant Limited is established in Kenya, you may also lodge a complaint with the Office of the Data Protection Commissioner of Kenya. The ODPC provides complaint channels at www.odpc.go.ke and lists its office at Britam Towers, 12th Floor, Hospital Road, Upper Hill, Nairobi, Kenya.

Contlant Limited**Company registration number: PVT-DLUP8X5A****Registered address: Muthithi Road, Westlands, Nairobi, Kenya****Email: privacy@contlant.com****Telephone: +254 780 074 521**

As a company incorporated in Kenya, Contlant is subject to applicable Kenyan law, including the Constitution of Kenya, the Data Protection Act, 2019, the Data Protection (General) Regulations, 2021 and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021. Depending on the location of a customer or individual and the nature of the processing, additional laws may apply, including the EU GDPR, the UK GDPR, Swiss data-protection law, US state privacy laws and comparable legislation in other countries. We will address mandatory local requirements through this policy, a regional notice, the customer agreement, data-processing terms or another appropriate safeguard.