Privacy Policy

1. About This Policy

Subcontext Ltd ("Subcontext", "we", "us" or "our") is a company registered in England and Wales (Company No. 17019645) with its registered office at 124 City Road, London, EC1V 2NX. We are registered with the Information Commissioner's Office (ICO) under reference ZC098511.

This Privacy Policy explains how we collect, use, share and protect personal data in connection with the Subcontext platform, apps, websites and services (the "Service"), as required by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (PECR).

It covers:

- people who use the Service on behalf of our business customers ("Customers"), such as owners, managers and users of a Customer's Organisation, and billing contacts;
- visitors to subcontext.com, people who chat with our own website assistant, people who ask us for a call or demo, and prospective customers we contact;
- financial advisers who use Nurture with AI through one of our partners; and
- in outline only, the individuals Customers communicate with through the Service ("Contacts"). For Contacts, Subcontext acts as a processor (see Section 2.2).

This Privacy Policy is an information notice. It is not part of any contract with us. The contract terms are our Terms of Service and, for personal data we process for Customers, our Data Processing Agreement. Please also see our Cookie Policy, Acceptable Use Policy and Consumer Notice.

2. Our Role: Controller or Processor

2.1 Where Subcontext Is the Controller

We decide why and how the following personal data is used, so we are its controller:

- **Account and user data:** the people who sign up for and use the Service, their sign-in, security and membership details.
- **Billing data:** billing contacts, payment and credit records, invoices.
- **Support:** support tickets, emails and calls with our team.
- **Our own website and website assistant:** visitors to subcontext.com, people who chat with the Subcontext assistant on our website, and people who submit our "Book a call" form. When you chat with our assistant, Subcontext is the business running it, so where the Consumer Notice refers to "the Provider", that is us.
- **B2B marketing:** our communications with existing and prospective business customers.
- **Security and operations:** logs and records we keep to secure, run and fix the Service.

- **Nurture with AI advisers:** adviser and firm identifiers we receive from partners, and records of advisers accepting our terms.

2.2 Where Subcontext Is a Processor

Customers use the Service to talk to and manage their own customers and prospects (Contacts) by web chat, SMS, WhatsApp, email and voice, and to quote, sell and administer insurance. For that Contact data, the Customer is the controller and Subcontext is its processor. We process it only on the Customer's instructions under the Data Processing Agreement.

If you are a Contact, the business you dealt with is responsible for your personal data. Its own privacy notice tells you how it uses your data and on what lawful basis, and our Consumer Notice explains how the Subcontext platform handles your information on that business's behalf. Section 10.2 explains how to exercise your rights.

Section 3.8 summarises the Contact data we process as a processor, for transparency. The rest of this policy (lawful bases, retention and sharing) is about data we control, unless it says otherwise.

2.3 Contacting Us About Data Protection

For any data protection question or request:

Subcontext Ltd, Data Protection 124 City Road, London, EC1V 2NX Email: hello@subcontext.com

3. Personal Data We Collect

3.1 Account and User Data

- **Identity:** first name, last name, display name, photo (if you add one), job role
- **Contact details:** work email address and, if you add them, phone numbers and other contact methods, with their verification status
- **Credentials:** your password (stored only as a one-way hash), two-factor authentication secrets and backup codes (stored encrypted)
- **Organisation and membership:** the Organisations you belong to, your role (owner, manager or user), your status and invitations
- **Preferences:** notification settings and other settings you choose
- **Legal acceptances:** which version of which legal document you accepted, when, and the IP address and browser used

3.2 Billing and Payment Data

- **Subscription:** plan, billing cycle, the price agreed
- **Payments:** card and Direct Debit payments are handled by Stripe. We do not see or store full card numbers. Where an Organisation pays by Bacs Direct Debit, the bank details are stored encrypted.
- **Transaction records:** amounts, dates, status, invoice and credit note references, billing contact, VAT number where given
- **Prepaid credit:** the Organisation's credit balance and each movement on it (allowance, top-ups, usage charges, adjustments and refunds), with the name of the person who bought a top-up

3.3 Support and Communications With Us

The content of support tickets, emails and calls with our team, and anything you choose to share in them.

3.4 Our Website, Website Assistant and Enquiries

- **Website assistant:** the messages you exchange with our assistant, any details you give it (such as your name, email address, phone number or company), the page you were on, and your IP address and browser details
- **"Book a call" form:** name, company, work email, phone number (optional), role, reason for getting in touch, IP address and browser details
- **Website visits:** for each page of subcontext.com we serve, the page, the referring website (without its query string), the time, and a pseudonymous visitor code made by hashing your IP address and browser details. We count visits on our servers: no cookie or tracking script is used for this.
- **Technical data:** see Section 3.5 and our Cookie Policy

3.5 Technical, Usage and Security Data

- **Device and connection:** IP address, browser and version, operating system, device type, time zone
- **Sessions:** your signed-in sessions, the device and browser each was opened from, and when each was last active
- **Security events:** sign-in attempts (successful and failed), account lockouts, two-factor authentication events, sign-in approvals
- **Audit log:** significant actions in the Service, recording who did what, to which record, when, from which IP address and browser, and, where a Subcontext administrator acted, which administrator
- **Usage Data:** operational metrics such as message and call volumes, response times, AI and channel costs and errors, and the pages and features used
- **Logs:** API and webhook request logs, integration logs, AI call logs (the model used, token counts, timings, costs and the prompts and outputs), error reports and performance traces
- **Dashboard assistant:** what you ask Subcontext's assistant in the dashboard, its replies, and the actions it proposed and you approved or declined

3.6 The Subcontext Apps

When you use a Subcontext app for iPhone, iPad, Mac or Android, or for Windows or Linux if we offer one (each an "App"), we also process:

- **Push notification data:** the push token issued for your device (by Apple's Push Notification service on Apple devices, or by Google's Firebase Cloud Messaging on Android), the device's name, the App's version, and when the device last used the Service. We use these only to deliver the notifications you have chosen to receive, and stop sending to a device when it signs out, its sign-in is revoked or expires, or Apple or Google tells us the token is no longer valid.
- **Notification content:** notifications carry a title, a short preview (which may include a Contact's name or part of a message) and a link to the relevant screen, and pass through Apple's or Google's notification service to reach your device.
- **Crash reports (Android):** if the Android App crashes or hits a serious error, it sends a report to Google's Firebase Crashlytics: the technical details of the error, the device model, the Android version,

memory and disk state, the App's version, and an identifier for that installation of the App. Reports do not include your name, email address or the content of your Organisations' conversations, and are used only to find and fix faults.

The App also keeps some data on your device, which does not leave it:

- **Your sign-in:** kept in the device's secure storage (the keychain on Apple devices, encrypted storage on Android), never synced to other devices or included in backups. Pages of the Service shown inside the App use the App's own web storage, which is cleared when you sign out.
- **Copies of what you have viewed:** so screens open quickly and can be read without a connection, the App keeps the most recent copy of the lists and records you have opened (which may include Contact personal data). This copy is protected by the device's data protection, excluded from device backups, limited in size, and deleted when you sign out of the App or delete your account.
- **Caller ID entries:** if you turn on caller ID, the App copies the names and phone numbers of your Organisations' Contacts to the device, so an incoming call from a Contact shows who is calling. On Android these are kept in a contacts account belonging to the App; on iPhone they are given to the device's call identification. They are removed when you turn caller ID off or sign out. The App does not read or upload the other contacts on your device.

The Apps do not use advertising identifiers and do not track you across apps or websites owned by other companies. If we release an App for Windows or Linux, this section applies to it. Before it processes any data not described here, we will update this policy.

3.7 Where Personal Data Comes From

- **From you:** when you sign up, use the Service, contact us, chat with our website assistant or fill in a form.
- **From your Organisation:** when an owner or manager invites you, they give us your name and email address and choose your role.
- **From partners:** for Nurture with AI, the partner whose software the adviser uses (such as Iress) sends us the firm's and adviser's identifiers, and the adviser's name and email address, so we can open and link the workspace.
- **From Google:** when you connect Google Calendar or Google Sheets, Google tells us the email address of the Google account you connected (see Section 6.5).
- **From Stripe:** payment status, and the type and last four digits of a card or the bank account used, for our records.
- **From the Service itself:** technical, usage and security data generated as you use it.

3.8 Contact Data We Process for Customers (as Processor)

For transparency, when Customers use the Service, we process on their behalf:

- **Conversations and messages** on web chat, SMS, WhatsApp and email, including attachments
- **Voice calls:** call audio processed in real time, call recordings (where the Customer enables them) and transcripts
- **Contact records:** names, email addresses, phone numbers, addresses, external identifiers, notes, CRM activity and outreach history

- **Insurance data:** quotes, applications, policies and claims, which can include date of birth, address, occupation, financial details and health information about the people to be insured, including children named on a policy
- **Payment data:** payment status from Stripe, and Bacs Direct Debit bank details stored encrypted
- **Visit details:** the page a conversation or form started from (its address with personal details removed, its title, and any campaign or advert parameters such as utm_source or an ad click identifier), the referring page without its query string, language and time zone, and a picture of that public page rendered by our own systems without the visitor's cookies, which never shows their personal information
- **Consent records:** each decision a Contact makes, or a Customer records for them, about being contacted: the purpose, the channel, the lawful basis, the exact wording shown, where and when it was given, and supporting evidence such as IP address and browser
- **Suppression digests:** when a Customer erases a Contact who had refused or withdrawn consent, a keyed one-way digest of their email address or phone number (never the address or number itself), so their objection is applied again if the same details are added later
- **Vulnerability flags and escalations:** signs that a person may be vulnerable, and conversations handed over to the Customer's team
- **Data from the Customer's integrations**, such as Google Calendar and Sheets, and the inputs and outputs of tools its AI agents use

The Customer decides the purposes and lawful bases for this data. Our commitments for it are in the Data Processing Agreement.

3.9 Whether You Have to Give Us Personal Data

You need to give us your name, a work email address and a password to have an account, and billing details for your Organisation to pay for the Service. Without them we cannot provide the Service. Everything else, such as a photo, extra contact methods or what you tell our website assistant, is up to you. You do not have to fill in our "Book a call" form or chat with our assistant, but we cannot reply to you without a way to reach you.

4. How We Use Personal Data and Our Lawful Bases

4.1 Purposes, Lawful Bases and Retention

This table covers personal data for which Subcontext is the controller. Where we rely on legitimate interests (UK GDPR Article 6(1)(f)), we have balanced our interest against your rights and expectations, and you can ask us for details of that assessment.

Purpose	Personal data	Lawful basis	Our legitimate interest (where relied on)	Retention
Creating and running user accounts: sign-up, invitations, sign-in, two-factor authentication, roles and Organisations	Account and user data (3.1), sessions and security events (3.5)	Legitimate interests. Contract (Article 6(1)(b)) where you contract with us yourself, for example as a sole trader	Giving the people our Customer authorises access to the Service the Customer has contracted for	While your account exists. When you delete your account, the details that identify you are erased straight away (see Section 10.1). When an Organisation's agreement ends, its data is deleted within 90 days of the Termination Date (Section 8.2)
Providing the Service to Customers, including the dashboard assistant, integrations, the API and the Apps	Account data (3.1), Usage Data and logs (3.5), app data (3.6)	Contract with the Customer; for its users, legitimate interests	Performing our contract with the Customer and supporting the people who use it	As for accounts, and the log periods in Section 8.1
Billing, payments, prepaid credit, invoicing and tax	Billing data (3.2), billing contacts' names and emails	Contract with the Customer; legal obligation (Article 6(1)(c)) for accounting and tax records; legitimate interests for billing contacts	Getting paid, and contacting the right person about bills	7 years from the end of the financial year the record relates to
Customer support	Support data (3.3), account and technical data needed to investigate	Legitimate interests	Helping Customers and their users and fixing problems they report	While the Organisation's account exists, then under the Termination Date clock (Section 8.2)
Service messages: security alerts, password resets, invitations, billing notices, notice of changes to our legal documents	Name, email address, the message and its delivery status	Legitimate interests; legal obligation where we must tell you something	Running the Service securely and keeping Customers informed	Email send and delivery logs: 2 years
Recording acceptance of our legal documents	Legal acceptances (3.1)	Legitimate interests	Being able to show which terms applied and who accepted them	For the life of the account and 6 years after the Organisation's agreement ends, to deal with legal claims

Purpose	Personal data	Lawful basis	Our legitimate interest (where relied on)	Retention
Security, fraud and abuse prevention: rate limiting, lockouts, investigating suspicious activity, admin access records	Security events, sessions, audit log, IP addresses, browser details (3.5)	Legitimate interests; legal obligation to keep personal data secure	Protecting the Service, Customers and the people they serve	Audit log: 2 years. Signed-in sessions expire after 30 days of inactivity and their records are deleted 1 year after they end. Firewall and server logs: 30 days. API request logs: 3 months
Running, monitoring and fixing the Service	Error reports, performance traces, AI call logs, integration logs (3.5), Android crash reports (3.6)	Legitimate interests	Keeping the Service working, reliable and cost-effective	Error reports: 90 days. Performance traces: 30 days. AI call logs: 13 months. Integration logs: 90 days. Android crash reports: 90 days
Planning, pricing and improving the Service	Usage Data (operational metrics only: volumes, latency, costs, errors)	Legitimate interests	Understanding how the Service is used so we can plan capacity, set prices and improve features. We never use Customer Content or Contact data to train AI models (Section 5.2)	Usage charges are billing records (7 years)
Measuring visits to our website	Website visit records (3.4)	Legitimate interests	Knowing which pages people read and where visitors come from, without cookies or tracking scripts	1 year
App notifications and crash reports	Push notification data and crash reports (3.6)	Legitimate interests	Delivering the notifications you have chosen and fixing App faults	Push tokens: until the device signs out, its sign-in is revoked or expires, or Apple or Google reports the token invalid. Crash reports: 90 days
Our own website assistant	Website assistant data (3.4)	Legitimate interests	Answering visitors' questions about Subcontext and showing how our product works	2 years after the conversation's last message
Responding to "Book a call" requests and other enquiries	Form data (3.4), emails you send us	Legitimate interests	Replying to people who ask to hear from us, and dealing with business enquiries	2 years after our last contact, unless you become a Customer

Purpose	Personal data	Lawful basis	Our legitimate interest (where relied on)	Retention
B2B marketing to existing and prospective business customers	Name, work email, phone, company, role, how you engaged with us	Legitimate interests, and consent where PECR requires it (Section 4.2)	Telling businesses about our services	Until you object or unsubscribe, or 2 years after your last engagement with us. We keep a minimal record of an objection so we can respect it
Nurture with AI: opening and linking adviser workspaces, and recording acceptance of the Nurture terms	Firm and adviser identifiers, adviser name and email (3.7), terms acceptances with IP address and browser	Legitimate interests; contract where the adviser's firm contracts with us	Providing the Nurture service the adviser asked for through the partner	An unclaimed trial workspace is deleted, with its contacts and conversations, after 90 days in which no message has been sent from it. Otherwise as for account data
Google Calendar and Sheets connections	Google account email address and access tokens (Section 6.5)	Legitimate interests	Providing the integration the Customer chose to connect	Until the connection is removed, or the Organisation's data is deleted
Legal and regulatory requirements, and legal claims	Any of the above, as needed	Legal obligation; legitimate interests	Establishing, exercising or defending legal claims, and responding to lawful requests	As long as the obligation or claim requires, including under a legal hold
Selling or reorganising our business	Any of the above, as needed	Legitimate interests	Allowing a buyer or successor to continue the Service	For the duration of the transaction

4.2 Direct Marketing and Your Right to Object

You can object to direct marketing at any time, and we will stop. Use the unsubscribe link in any marketing email, or email hello@subcontext.com. This right is absolute: we do not need a reason.

We send B2B marketing only to business contacts. Under PECR:

- for people at companies, limited liability partnerships and government bodies ("corporate subscribers"), we may send marketing emails relying on legitimate interests, always identifying ourselves and offering an easy way to opt out;
- for sole traders and some partnerships ("individual subscribers"), we send marketing emails only with your consent, or where you are an existing customer or asked us about our services, the message is about similar services, and you were given a chance to opt out when we collected your details and in every message since (the "soft opt-in"); and
- we do not make marketing calls to numbers registered with the Telephone Preference Service or Corporate Telephone Preference Service without permission.

Service messages (Section 4.1) are not marketing and continue while you have an account.

4.3 Consent

Where we rely on consent, you can withdraw it at any time, as easily as you gave it, by using the link in the message or emailing hello@subcontext.com. Withdrawing consent does not affect processing that took place before you withdrew it.

4.4 Special Category Data

As controller, we do not ask for special category data (such as health information). If you include it in a support ticket or a chat with our website assistant, we use it only to deal with your request.

Contact data processed for Customers can include health information, for example in insurance applications. The Customer, as controller, is responsible for the conditions under UK GDPR Article 9 that permit it.

5. AI and Automated Decision-Making

5.1 How the Service Uses AI

- **For Customers (as processor):** AI agents hold conversations with Contacts, screen messages against safety and compliance rules, detect when a person needs a human, propose and carry out the actions the Customer has allowed, and summarise conversations.
- **Our dashboard assistant (as controller of your prompts):** Subcontext's assistant in the dashboard answers questions and proposes actions. Every change it proposes needs a user's approval before it happens.
- **Our website assistant (as controller):** answers visitors' questions on subcontext.com.

5.2 AI Providers, Data Retention and Training

Text AI runs on Amazon Web Services (AWS) Bedrock in the EU (requests go to Ireland and may be served from another AWS EU region) or London, using Anthropic (Claude) and DeepSeek models. AWS Bedrock does not store prompts or responses, or use them to train models.

Voice calls use OpenAI for real-time speech, transcription and speech synthesis, and ElevenLabs for speech synthesis, both in the United States. OpenAI does not train its models on data sent through its API, but may keep it for up to 30 days to monitor for abuse.

Subcontext does not use Customer Content or Contact personal data, whether or not anonymised, to train or fine-tune any AI model.

5.3 Automated Decisions and Profiling

The Service makes some automated assessments when Customers use it:

- **Content screening:** messages are checked against safety and compliance rules, and may be blocked or flagged.
- **Escalation detection:** conversations that need a person are handed to the Customer's team.
- **Action approvals:** an agent's proposed action is allowed, held for human approval or refused under the Customer's rules.
- **Vulnerability detection:** the Service looks for signs that a person may be vulnerable (for example signs of financial difficulty, illness, bereavement or confusion). Where it finds them, it flags the person,

holds back sales and outreach to them, and alerts the Customer's team. This is profiling and may involve inferring information about a person's health.

- **Lead scoring and routing:** where the Customer uses the CRM, leads may be scored and prioritised under the Customer's rules.

These features run on the Customer's instructions and support the Customer's own decisions. Whether any decision about a Contact has legal or similarly significant effects (for example, whether to offer insurance, or on what terms) depends on how the Customer uses the Service, and is the Customer's responsibility as controller, including providing human review and explaining people's rights under UK GDPR Article 22. Insurance prices and underwriting decisions come from insurers and the Customer's own rules, not from Subcontext.

Subcontext does not make decisions about its own users or website visitors based solely on automated processing that have legal or similarly significant effects. Automated security measures, such as locking an account after repeated failed sign-ins, are temporary and can be reviewed by contacting us.

6. Who We Share Personal Data With

6.1 We Do Not Sell Personal Data

We do not sell, rent or trade personal data, and we do not share it with third parties for their own marketing.

6.2 Our Service Providers

We use service providers (sub-processors) to host and run the Service. For data we control, they include: AWS (hosting, storage, email delivery and AI on Bedrock), Stripe (payments), Twilio (SMS and phone verification codes), Apple and Google Firebase (App notifications and Android crash reports), and Google (Calendar and Sheets, where a Customer connects them). They act on our instructions under written contracts.

The full, current list of the sub-processors we use for the Service, with their locations and purposes, is in section 6.1 of our Data Processing Agreement and at /trust/sub-processor-list.

6.3 Organisations That Act as Independent Controllers

Some organisations we work with decide for themselves how they use the data they receive, under their own privacy notices:

- **Stripe** acts as an independent controller for some payment data, for example to prevent fraud and meet its legal obligations as a payment provider.
- **Apple and Google** operate the notification services that deliver App notifications, and their app stores.
- **Meta (WhatsApp)** processes WhatsApp messages under its own terms when a Customer uses WhatsApp.
- **Google and Meta advertising:** where a Customer connects its own advertising account, the Service reports conversions to it on the Customer's instructions. Google and Meta handle that data under their terms with the Customer. We do not do this for our own marketing.
- **Our professional advisers** (lawyers, accountants, auditors and insurers), who are bound by confidentiality.

6.4 Other Disclosures

- **Law enforcement, regulators and courts:** we disclose personal data we control where the law requires it, or where we reasonably believe it is necessary to prevent crime, protect someone's safety or establish, exercise or defend legal claims. For data we process for Customers, we follow the Data Processing Agreement: we tell the Customer about a binding request unless the law forbids it, and disclose only the minimum required.
- **Business transfers:** if we sell, merge or reorganise our business, personal data may pass to the buyer or successor, who must protect it as this policy describes. We will tell affected Customers.

6.5 Google User Data (Google Workspace Integrations)

Customers may connect Google Calendar and Google Sheets to their Organisation for appointment scheduling and record export. Where a Customer authorises these integrations through Google's consent screen, we access the following Google user data, only to provide those features:

- **Google account email address:** shown in the Service so authorised users can see which Google account a connection belongs to.
- **Google Calendar data** (free and busy information, the account's calendar list, and calendar events): used to check availability and to create, update or cancel the appointments booked through the Service, including sending calendar invitations and, where enabled, Google Meet links.
- **Google Sheets and Drive file data:** used to create spreadsheets, list spreadsheets created by the Service or chosen by the user, read worksheet names, and add appointment records as rows to a spreadsheet the Customer selects.

Access and refresh tokens are stored encrypted and used only to make the calls described above. Request and response details are kept in integration logs for 90 days so Customers can check the integration's activity. We do not use Google user data to develop, improve or train generalised artificial intelligence or machine learning models.

Access can be revoked at any time by disconnecting the integration in the Service or in your Google account settings. When access is revoked, we stop using the stored tokens straight away.

Subcontext's use and transfer to any other application of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. In particular, we do not sell Google Calendar or Sheets data, we do not use it for advertising, and we do not let people read it except with the user's agreement, where necessary for security or to comply with the law, or where the data has been aggregated and anonymised. Separately from this integration, a Customer may connect a Google Ads account for conversion reporting (Section 6.3); Google Calendar and Sheets data is never used for that.

6.6 Connected Advertising Accounts

Customers may connect a Google Ads or Meta advertising account to their Organisation. Through Google's or Meta's sign-in, we read the account's list of ad accounts, its campaign names, daily spend, impressions and clicks, and the names of its conversion actions or pixels. We use this only to show the Organisation its advertising cost against the business it produced, and to report the conversions it chooses (Section 6.3). Access tokens are stored encrypted, and request and response details are kept in integration logs for 90 days so Customers can check the activity. We do not use this data for our own

advertising. The Customer can disconnect the account at any time in the Organisation's integration settings, after which we stop all access.

7. Where Personal Data Is Processed and International Transfers

Platform data is hosted by AWS in Ireland (eu-west-1). Text AI runs on AWS Bedrock in the EU (Ireland, eu-west-1, whose EU cross-region routing may serve a request from another AWS EU region) or London (eu-west-2). Voice AI (OpenAI and ElevenLabs), messaging (Twilio and Meta), payments (Stripe) and App notifications (Apple and Google Firebase) involve providers in the United States.

The UK recognises the European Economic Area as providing adequate protection. For transfers to the United States, we rely on the UK Extension to the EU-US Data Privacy Framework (the "UK-US data bridge") where the recipient is certified, and otherwise on the UK International Data Transfer Agreement or the EU Standard Contractual Clauses with the UK Addendum. We also use encryption in transit and at rest.

Our Transfer Risk Assessment is published at /trust/transfer-risk-assessment, and the location of each sub-processor is in our Data Processing Agreement. You can ask us for a copy of the safeguards that apply to a transfer by emailing hello@subcontext.com.

8. How Long We Keep Personal Data

8.1 Data We Control

The retention period for each purpose is in the table in Section 4.1. In summary, the periods applied automatically by the Service are:

Record	Retention
Audit log	2 years
Email send and delivery logs	2 years
Website visit records	1 year
Signed-in sessions	Expire after 30 days of inactivity; records deleted 1 year after they end
AI call logs	13 months
API and webhook request logs	3 months
Integration logs	90 days
Error reports	90 days
Performance traces	30 days
Firewall and server logs	30 days
Payment provider event records	7 years
Data exports you download	File deleted after 7 days
Unclaimed Nurture with AI trial workspaces	Deleted after 90 days in which no nurture has been sent

Record	Retention
Android App crash reports (Firebase Crashlytics)	90 days

The periods in Section 4.1 for legal acceptances, our website assistant, enquiries and B2B marketing are applied by periodic review rather than automatic deletion.

8.2 When a Customer's Agreement Ends

The Customer may export its data, or ask for it to be returned or deleted, within 30 days of the Termination Date (the date its subscription or agreement ends, as defined in the Terms of Service). We delete the Customer's data within 90 days of the Termination Date, and automated database backups expire within 7 days after that. We keep some records longer, only where listed:

- billing and payment records: 7 years, because the law requires it;
- the compliance decision trail: for the retention period the Customer configured (6 years by default), where the Customer instructs it or the law requires it;
- the audit log: 2 years; and
- anything under a legal hold.

8.3 Contact Data We Process for Customers

Customers decide how long Contact data is kept. Some periods are set by the Customer in the Service, for example voice call recordings (365 days by default, or never deleted automatically if the Customer sets zero), raw lead submissions (365 days by default) and the compliance decision trail (6 years by default, between 3 and 25 years). The raw copies of inbound emails received for a Customer are deleted from storage after 30 days. Other Contact data is kept until the Customer deletes it or its agreement ends (Section 8.2). Our retention commitments to Customers are in the Data Processing Agreement.

9. Security

We protect personal data with technical and organisational measures, including:

- **Encryption:** TLS 1.2 or higher in transit; the whole database encrypted at rest; sensitive fields (such as two-factor secrets, integration credentials and Direct Debit bank details) additionally encrypted with AES-256-GCM
- **Access control:** owner, manager and user roles, with each Organisation's data kept separate; two-factor authentication enforced by default for new Organisations
- **Sessions:** sessions you can see and end from your profile, which expire after 30 days of inactivity; changing your password or turning off two-factor authentication ends your other sessions; each App's sign-in is tied to a session you can revoke
- **Audit trail:** an audit log that cannot be edited, recording significant actions, including any action taken by a Subcontext administrator
- **Infrastructure:** hosting on AWS in private networks, with a web application firewall, rate limits and managed secrets
- **Incident response:** procedures for identifying, containing and fixing incidents, and for notifying the ICO, Customers and affected people where the law requires

More detail is in our published security policies at /trust. No system is completely secure, but we work to keep the risk as low as reasonably possible.

10. Your Rights

10.1 Rights Over Data We Control

Under the UK GDPR you have the right to:

- **Access:** get a copy of the personal data we hold about you
- **Rectification:** have inaccurate or incomplete data corrected
- **Erasure:** have your data deleted in certain circumstances
- **Restriction:** ask us to limit how we use your data in certain circumstances
- **Portability:** receive data you gave us in a structured, commonly used, machine-readable format, where we process it by consent or contract
- **Objection:** object to processing based on legitimate interests, and to direct marketing at any time (Section 4.2)
- **Withdraw consent:** where we rely on consent (Section 4.3)
- **Automated decisions:** not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects on you

You can delete your own account at any time, from your profile on the website or from Account, then Delete account, in any App. This signs you out everywhere (including the App on every device), removes you from every Organisation and erases the personal details that identify you: your name, email address, photo, two-factor authentication secrets, contact methods and notification settings. Records we or our Customers need to keep, such as messages you sent on a Customer's behalf, escalations you handled, your acceptance of our terms, and audit log entries (which may include IP addresses), are kept for their normal retention period and attributed to a deleted user.

To exercise your rights, email hello@subcontext.com. We will reply within one month. We may extend this by up to two further months for complex or numerous requests, and will tell you within the first month if we do. We may need to confirm your identity first.

10.2 If You Are a Contact

If you have dealt with a business that uses Subcontext (for example, you chatted with its AI agent, received a message from it or applied for insurance through it), that business controls your data. Please send requests to it first: its privacy notice explains how. We help our Customers respond to requests under the Data Processing Agreement.

If you send a request to us, we will pass it to the business concerned without undue delay and tell you we have done so. If you cannot identify or reach the business, email hello@subcontext.com and we will help where we can.

10.3 Complaints

If you are unhappy with how we have handled your personal data, please contact us first at hello@subcontext.com. You also have the right to complain to the Information Commissioner's Office:

Information Commissioner's Office ico.org.uk Helpline: 0303 123 1113

11. Children

Our Service is for businesses. Users of the Service must be 18 or over, and our website and website assistant are not aimed at children.

Customers may process information about children through the Service, for example where a child is named as an insured person on a policy. The Customer is responsible for having a lawful basis for that processing and for complying with the ICO's Age Appropriate Design Code (Children's Code) where it applies.

12. Third-Party Websites and Embedded Content

Our websites and the Service may link to other websites, and some pages show content from other providers, such as fonts from Google Fonts and YouTube or Vimeo videos. Those providers may receive your IP address and browser details, and may set their own cookies. Our Cookie Policy explains which pages use them. Please read the privacy notices of any third-party service you use.

13. Changes to This Policy

This policy is an information notice, and we update it when our processing changes. Where a change is material, we will tell Customers by email or with a notice in the Service at least 30 days before it takes effect, unless the change is needed sooner to comply with the law. The version number and publication date shown with this document identify the current version.

14. Contact

For all privacy and data protection enquiries:

Subcontext Ltd Registered in England and Wales, No. 17019645 ICO registration No. ZC098511 124 City Road, London, EC1V 2NX Email: hello@subcontext.com

Subcontext Ltd, registered in England and Wales, Company No. 17019645. Registered office: 124 City Road, London, EC1V 2NX. The current version of this document is published at subcontext.com.