Terms of Service

1. About these Terms

1.1 The Parties

These Terms of Service ("Terms") are an agreement between Subcontext Ltd ("Subcontext"), a company registered in England and Wales (Company No. 17019645) whose registered office is at 124 City Road, London, EC1V 2NX, and the business, firm or other organisation that signs up for or uses the Service ("Customer").

1.2 Acceptance

Customer accepts these Terms when a User creates an Organisation, accepts these Terms in the Service, signs an Order Form that refers to them, or first uses the Service on Customer's behalf, whichever happens first. A User who accepts these Terms (or the Acceptable Use Policy or the Data Processing Agreement) accepts them on Customer's behalf and confirms that they are authorised to do so. If Customer does not agree to these Terms, it must not use the Service.

1.3 Business Use

The Service is provided for business purposes only. Customer acts for the purposes of its trade, business or profession, and this Agreement is not a consumer contract. Every User must be at least 18 years old. Customer is responsible for every User and for everyone else who uses the Service through Customer's Organisations, including its employees, contractors and agents.

2. Definitions and Interpretation

2.1 Definitions

In these Terms:

- **"Acceptable Use Policy"** or **"AUP"** means Subcontext's Acceptable Use Policy.
- **"Account"** means an individual User's login to the Service. An Account may belong to one or more Organisations.
- **"Agent"** means an AI agent that Customer creates and configures in the Service to converse with Contacts and to take actions through Tools.
- **"Agent Output"** means any text, speech, data, decision, action or other output generated by an Agent, including messages sent to Contacts, records created or changed, and Tools invoked. Agent Output does not include the Service itself.
- **"Agent Policy"** means a set of rules that Customer applies to Agents to screen content, detect when to escalate, and require approval before actions.
- **"Agreement"** means these Terms together with the other documents listed in Section 23.1.
- **"App"** has the meaning given in Section 3.5.

- **"Billing Period"** means the recurring period (monthly, unless otherwise agreed) for which subscription Fees are charged.
- **"Bought Credit"** means Credit that Customer buys as a top-up, or that Subcontext adds to an Organisation's balance.
- **"Confidential Information"** has the meaning given in Section 20.1.
- **"Contact"** means an individual or organisation with whom Customer communicates or whose information Customer processes through the Service, including Customer's own customers, prospects, applicants, policyholders, claimants, callers and message recipients.
- **"Context Block"** means a knowledge source that Customer configures for use by Agents.
- **"Conversation"** means a sequence of messages or a call between an Agent or a User and a Contact on any channel.
- **"Credit"** means the prepaid balance, in pounds sterling, from which an Organisation billed for usage by Credit pays its usage-based charges. It is made up of Included Credit and Bought Credit.
- **"Customer Content"** means the content that Customer and its Users create, upload or configure in the Service, including Context Blocks, Agent configuration and instructions, templates, Agent Policies, Consent Rules, and hosted pages and forms.
- **"Customer Data"** means all data, including personal data, that Customer, its Users or its Contacts submit to the Service, or that the Service generates for Customer in operating its Organisations, including Customer Content, Conversations, Agent Output, Contact records, Consent Records, call recordings and transcripts, and insurance quote, application, policy, claim and payment records. Customer Data does not include Usage Data or the account, billing and security records that Subcontext keeps for its own purposes as described in the Privacy Policy.
- **"Dashboard Assistant"** means Subcontext's own AI assistant in the Service's dashboard, described in Section 6.5.
- **"Data Processing Agreement"** or **"DPA"** means Subcontext's Data Processing Agreement.
- **"Documentation"** means the user guides, help pages, feature descriptions and API references for the Service that Subcontext makes available in the Service or on subcontext.com, as updated from time to time.
- **"Fees"** means the amounts payable for the Service: subscription fees, usage-based charges, purchases of Credit, and any other charges set out in these Terms or an Order Form.
- **"Fixed Term"** means a minimum or fixed period for a Subscription agreed in an Order Form (for example twelve (12) months), including any renewal term the Order Form provides for.
- **"Guardrail"** means a control that screens or restricts Agent behaviour, including the baseline guardrails Subcontext applies to every Agent and the guardrails, conduct rules and Agent Policies that Customer configures.
- **"Included Credit"** means the Credit that a Plan grants an Organisation each calendar month.
- **"Order Form"** means an order form, Enterprise agreement or other written agreement for the Service that refers to these Terms and is signed by both parties.
- **"Organisation"** means a workspace in the Service belonging to Customer, which is the boundary for data isolation, billing and access control. Customer may have more than one Organisation.
- **"Personal Data Breach"** has the meaning given in the DPA.

- **"Plan"** means a subscription tier (such as Starter, Professional, or an individually agreed Enterprise plan) with the features, usage allowances and pricing described in the Service or in an Order Form.
- **"Regulated Customer"** has the meaning given in Schedule 1.
- **"Service"** means the Subcontext platform and related services that Subcontext provides to Customer, including the software, dashboard, Agents' runtime, channels, APIs, the MCP server, the Apps, the Dashboard Assistant and the Documentation.
- **"Subscription"** means Customer's purchase of a Plan for an Organisation, whether it renews each Billing Period or runs for a Fixed Term under an Order Form.
- **"Termination Date"** means the date on which this Agreement, or the Subscription for an Organisation, ends and access to the Service under it ceases. For a cancelled Subscription, that is the end of the Billing Period in which it was cancelled or, if earlier, the end of the grace period in Section 12.11. For a Subscription with a Fixed Term, it is the end of that Fixed Term, unless the Subscription ends earlier under this Agreement.
- **"Tool"** means a configured action that an Agent may invoke during a Conversation.
- **"Usage Data"** has the meaning given in Section 9.5.
- **"User"** means an individual whom Customer authorises to use the Service through an Account in one of Customer's Organisations.

Other terms are defined where they first appear.

2.2 Interpretation

In this Agreement: headings do not affect interpretation; "including" and similar words mean "including without limitation"; the singular includes the plural and the other way round; "writing" and "written" include email, except where a document must be signed by both parties (electronic signatures count as signatures); a reference to a statute or regulation is to it as amended, extended or re-enacted from time to time, and includes subordinate legislation made under it; a reference to a regulator's rules or guidance is to them as updated from time to time; and a reference to a Section or Schedule is to a section of, or schedule to, these Terms.

3. Accounts, Users and Access

3.1 Registration

Customer must ensure that the information it and its Users give when signing up, and the Organisation's business details, are accurate, complete and kept up to date. Giving false or misleading information about Customer's identity or business is a material breach of this Agreement.

3.2 Users and Account Security

Each Account is for one named individual and must not be shared. Customer is responsible for keeping credentials secure, including passwords, API keys, two-factor authentication devices, OAuth tokens and session tokens, and for everything done through its Users' Accounts and its Organisations. Customer must tell Subcontext without undue delay at hello@subcontext.com if it suspects unauthorised access to an Account or Organisation. Customer is not responsible for access that results from Subcontext's breach of its security obligations.

3.3 Organisations and Roles

An Organisation's owners and managers decide who joins it and what role each User has (owner, manager or user), and are responsible for the access they grant. Customer is responsible for the actions of all Users in its Organisations, including the content they create, the Agents they configure and the communications they start.

3.4 API, MCP and Third-Party Assistants

Use of the Service through its APIs is subject to this Agreement. Customer must not share API credentials outside its own business, exceed published rate limits, or use the API in a way that degrades the Service for other customers.

The Service can also expose an Organisation's Agents and Tools to third-party AI assistants and agent platforms (for example through the Model Context Protocol server, ChatGPT and Claude apps, and WebMCP tools embedded on Customer's website). Where Customer enables such an exposure, every action a third-party assistant takes through it is Customer's own use of the Service: Customer is responsible for the assistant's requests, for the data it is given, and for the tokens or credentials that authorise it, and must revoke them when they are no longer needed. Subcontext does not operate those third-party assistants and is not responsible for how they use what they are given.

3.5 The Subcontext Apps

Subcontext makes the Service available through applications for Apple iPhone and iPad, Apple Mac and Google Android devices, and may in future offer applications for Microsoft Windows and Linux (each an "App"). Each App is part of the Service and this Agreement applies to it. Subcontext grants each User a limited, non-exclusive, non-transferable, revocable licence to install and use the App on devices that the User or Customer owns or controls, solely to access the Service in accordance with this Agreement. Where the App is obtained from Apple's App Store, that licence is also limited to Apple-branded devices and to the uses permitted by the Usage Rules in the Apple Media Services Terms and Conditions. The App may be obtained only from Apple's App Store, Google Play, subcontext.com, or another store or repository that subcontext.com names as an official source.

The App signs in with a User's Account and stays signed in until the User signs out, the sign-in is revoked (a User can revoke it at any time under Sessions in their profile), or it goes unused for thirty (30) days. Anyone who can use an unlocked device can act as its User in the App, so Users must protect their devices with a passcode or biometric lock and sign out of the App before passing a device to someone else. The App can send push notifications about activity in a User's Organisations, which may show a Contact's name or a short preview of a message on the device's lock screen; Users choose which notifications they receive in their notification preferences and can turn them off in the device's settings.

Where a User turns it on, the App's caller ID feature copies the names and phone numbers of the Organisation's Contacts to the device, so that an incoming call from a Contact shows who is calling. On Android these entries are kept in a contacts account belonging to the App; on iPhone they are given to the device's call identification. The feature is off until the User turns it on, and the entries are removed when the User turns it off or signs out of the App. Customer must allow its Users to use the feature only where Customer's data protection obligations permit Contact details to be held on the device.

Where the App is obtained from Google Play, this Agreement is between Customer and Subcontext only, and not with Google LLC ("Google"); Subcontext, not Google, is solely responsible for the App, its content,

maintenance and support; and use of Google Play is also subject to Google's own terms of service.

Where the App is downloaded from subcontext.com (such as the Mac App, or a Windows or Linux App if one is offered), the licence above applies to that copy, and Users must install only copies obtained directly from subcontext.com. Where Subcontext makes a Windows or Linux App available through another store or package repository, this Agreement applies to it in the same way, together with any terms of that store that apply to the User.

Where the App is obtained from Apple's App Store:

- this Agreement is between Customer (and its Users) and Subcontext only, and not with Apple Inc. ("Apple"); Subcontext, not Apple, is solely responsible for the App and its content;
- Apple has no obligation to provide any maintenance or support services for the App;
- if the App fails to conform to any applicable warranty, the User may notify Apple and Apple will refund any purchase price paid for the App; to the maximum extent permitted by law, Apple has no other warranty obligation with respect to the App, and any other claims, losses, liabilities, damages, costs or expenses attributable to a failure to conform to a warranty are Subcontext's responsibility, subject to this Agreement;
- Subcontext, not Apple, is responsible for addressing any claims by Customer, a User or any third party relating to the App or its possession and use, including product liability claims, claims that the App fails to conform to a legal or regulatory requirement, and claims arising under consumer protection, privacy or similar legislation;
- if a third party claims that the App or its possession and use infringes that third party's intellectual property rights, Subcontext, not Apple, is solely responsible for the investigation, defence, settlement and discharge of that claim;
- Customer confirms that it and its Users are not located in a country that is subject to a UK, EU or US Government embargo or that has been designated by the US Government as a "terrorist supporting" country, and are not listed on any UK, EU or US Government list of prohibited or restricted parties;
- Users must comply with any applicable third-party terms (such as their mobile network provider's terms) when using the App; and
- Apple and its subsidiaries are third-party beneficiaries of this Agreement as it relates to the App, and on acceptance of these Terms Apple will have the right (and will be deemed to have accepted the right) to enforce them against Customer and its Users as a third-party beneficiary.

4. The Service

4.1 What the Service Does

The Service is a platform for UK insurers, brokers and other businesses to run AI Agents and the work around them. Depending on Customer's Plan, it includes: Agents that converse with Contacts by web chat (including the embeddable widget), SMS, WhatsApp, email and voice calls, and take actions through Tools; a CRM with leads, outreach campaigns and workflows; insurance quoting, applications, policies, claims and premium collection; payments through Stripe; integrations with Customer's and third parties' systems; hosted pages, forms and custom domains; a REST API and an MCP server; the Apps; and the Dashboard Assistant. The Documentation describes each feature. Subcontext will provide the Service in accordance with this Agreement and the Documentation.

4.2 Changes to the Service

Subcontext develops the Service continually and may add, change or remove features. Subcontext will not make a change during a Subscription that materially reduces the core functionality of Customer's paid Plan except in accordance with Section 12.12 or Section 21, or where a third-party provider or the law requires it (in which case Subcontext will give as much notice as is reasonably practicable).

4.3 Third-Party AI Models

The Service uses third-party AI models. Text models (Anthropic's Claude models and DeepSeek) run on Amazon Web Services' Bedrock service 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 calls use real-time speech, transcription and speech models from OpenAI and speech synthesis from ElevenLabs, which are provided from the United States. Platform data is hosted by Amazon Web Services in Ireland (eu-west-1); messaging (Twilio, Meta), payments (Stripe) and app push notifications (Apple, Google Firebase) also involve providers in the United States. The current providers are listed in the sub-processor list in section 6.1 of the Data Processing Agreement and at /trust/sub-processor-list, and transfers are protected as described in the DPA and the Transfer Risk Assessment at /trust/transfer-risk-assessment.

AWS Bedrock does not store prompts or responses or use them to train models. OpenAI does not train on data sent through its API but may retain it for up to 30 days for abuse monitoring. Subcontext does not use Customer Data, or personal data of Contacts, whether or not anonymised, to train or fine-tune any AI model.

Subcontext does not develop these models, and their providers may update them, which can change how Agents behave. Where a model is discontinued, deprecated or materially degraded by its provider, Subcontext may substitute a model of reasonably comparable quality and capability and will tell Customer about the substitution. Exact equivalence between models is not achievable, and minor differences in output are not a breach of this Agreement. Customer should test its Agents after a model change and adjust their configuration as needed.

4.4 Beta Features

Subcontext may offer features marked "beta", "preview", "experimental" or similar ("Beta Features"). Beta Features are offered for evaluation, may be changed or withdrawn at any time, and are not covered by the warranty in Section 14.2 or any service level. Customer should not rely on them for critical business processes.

4.5 Customer Default

If Subcontext's performance is prevented or delayed by an act or omission of Customer, its Users or its contractors (for example misconfigured Tools, invalid credentials, inaccurate data, or a lapsed third-party subscription that Customer is responsible for) ("Customer Default"), Subcontext is not liable for the resulting failure or delay, may suspend the affected part of its performance until the Customer Default is remedied, and Customer will reimburse Subcontext's reasonable, documented costs arising from the Customer Default.

4.6 What the Service Does Not Include

Unless an Order Form says otherwise, the Service does not include: legal, regulatory, compliance, financial or other professional advice; implementation consulting, bespoke development or other

professional services; or real-time synchronisation with external systems (data obtained from integrations may be cached and so may be out of date). The Service keeps backups of its database for recovery purposes (Section 10.4), but it is not Customer's system of record for regulatory record keeping, and Customer remains responsible for keeping, or exporting and keeping, the records it is required by law or its regulators to hold for longer than the retention periods it configures.

4.7 Subcontext's Compliance with Law

Subcontext will comply with the laws and regulations that apply to it in providing the Service.

5. Regulatory Responsibility

5.1 Customer's Regulatory Position

Many customers of the Service are authorised or regulated by the Financial Conduct Authority or the Prudential Regulation Authority. Customer is responsible for determining whether its use of the Service involves regulated activities, for holding and maintaining every authorisation, permission and registration its activities require, and for its compliance with the rules that apply to it, including the FCA's Principles, the Consumer Duty, the conduct of business rules, the financial promotion rules (including the approval of financial promotions), complaints handling, record keeping, and the rules on outsourcing and operational resilience. Customer remains the authorised firm responsible for its regulated activities when it uses the Service to carry them out.

5.2 Declaring Regulated Status

When it sets up an Organisation, or at any later time, Customer must declare in the Service (or, until the Service provides that setting, by email to hello@subcontext.com) whether it is authorised or regulated by the FCA, the PRA or another financial services regulator, and if so which regulator and its firm reference number, and must keep that declaration up to date. Once Customer has declared that it is regulated, or an Order Form says so, Customer is a Regulated Customer and Schedule 1 applies.

5.3 Compliance Features are Tools

The Service includes features designed to support Customer's compliance, including: conduct rules covering FCA conduct, the Consumer Duty, medical disclosure, vulnerable customers, complaints handling, financial promotions and data protection; vulnerability detection, which flags a Contact who may be vulnerable, holds back sales and outreach to them, and alerts Customer's team; complaints tracking with configurable acknowledgement and final response deadlines; a tamper-evident compliance decision trail; an AI disclosure rule; consent records and checks; human escalation and review; and approvals before Tools run. These features are tools that help Customer meet its obligations. They do not guarantee compliance, and Customer remains responsible for configuring them, for checking that they meet its own obligations, and for its own compliance oversight. Subcontext remains responsible for providing these features as described in the Documentation and applying them as Customer has configured them.

5.4 No Regulated Advice

Agents must not be configured or used to give regulated advice, meaning a personal recommendation on the merits of a particular insurance, investment or other financial product. Non-advised (information-only) insurance distribution is permitted, including providing product information, establishing a Contact's demands and needs, giving quotes, and taking applications, provided Customer complies with the rules

that apply to it. Where Agents communicate with Contacts in a way that is or contains a financial promotion, Customer is responsible for ensuring those communications comply with the financial promotion rules, including approval where it is required.

5.5 Subcontext's Regulatory Status

Subcontext does not hold an FCA or PRA authorisation, does not carry on regulated activities on Customer's behalf, and is not Customer's appointed representative, introducer or agent for regulatory purposes. Subcontext is a technology provider to Customer.

5.6 Restricted Use Cases

Without limiting the AUP, Customer must not configure or use Agents:

- to diagnose medical conditions, recommend treatments or triage patients (asking the health questions an insurance application requires, and recording the answers with the consent the Service supports, is permitted);
- to give specific legal advice or make legal determinations;
- to give regulated advice as described in Section 5.4;
- as the primary point of contact for emergencies where delay could endanger life or safety; or
- to control, or make decisions affecting, critical infrastructure, public utilities or safety-critical systems.

Where Customer uses the Service to make decisions based solely on automated processing that produce legal or similarly significant effects on individuals (for example automated underwriting decisions), Customer must ensure it has a lawful basis for doing so and provides the safeguards the law requires, including a way for the individual to obtain human review and contest the decision.

Where Agents interact with vulnerable individuals, children, or people in sensitive circumstances, Customer must ensure that Agents identify themselves as AI, offer a clear route to a person, and do not make or purport to make binding decisions affecting the individual without the safeguards described above.

6. AI Agents, Tools and the Dashboard Assistant

6.1 Configuring and Testing Agents

Customer decides what its Agents are used for and is responsible for creating, configuring, testing, deploying and monitoring them, including their instructions, Context Blocks, Guardrails, Agent Policies and Tools. The Service provides testing and compliance check tools; Customer must test each Agent before putting it live and after material changes to its configuration, and must maintain appropriate human oversight of Agents in operation.

6.2 Autonomous Operation

Once deployed, Agents generate responses, send messages, invoke Tools and take other actions without a person approving each one, except where Customer has configured an approval. By deploying an Agent, Customer authorises it to act within the parameters Customer has configured.

6.3 Guardrails

Subcontext applies baseline guardrails to every inbound message (screening for prompt injection, jailbreak attempts and attempts to extract an Agent's instructions), which Customer cannot detach, and separates untrusted content from Agent instructions. Customer configures further Guardrails, conduct rules and Agent Policies for its use case. Guardrails reduce the risk of undesirable Agent behaviour but cannot eliminate it, and the baseline guardrails may not be sufficient for Customer's particular use case, industry or regulatory requirements.

6.4 Tools and External Actions

By configuring a Tool and assigning it to an Agent, Customer authorises the Agent to invoke it. When a Tool calls an external service, the Service sends the request using the credentials, endpoints and parameters Customer has configured. Subcontext is not responsible for the availability, accuracy or behaviour of external services that it does not provide, or for authentication, rate limiting or blocking by them. Actions taken in external services may be irreversible, and the Service does not provide a general undo for them; Customer is responsible for configuring approvals, limits and monitoring for Tools whose actions could have significant consequences.

6.5 The Dashboard Assistant

Where it is enabled for an Organisation, the Dashboard Assistant is Subcontext's own AI in the dashboard. It answers questions about Customer's Organisation and proposes actions, and it acts only within the access of the User who is using it. Every action that would create, change, send or delete anything waits for that User's approval before it runs; an action the User approves is that User's action, and Customer is responsible for it as for any other action of a User. The Dashboard Assistant's answers and proposals can be wrong, and Section 6.7 applies to them as it does to Agent Output.

6.6 Escalation and Human Handover

The Service lets Agents hand Conversations to Customer's team, triggered by conditions an Agent detects, Agent Policy rules or a User. Customer is responsible for staffing its team and for responding to escalated Conversations in good time; Subcontext does not commit to any response time for them.

6.7 AI Output

AI output can be wrong, incomplete, out of date, biased or inappropriate, even when an Agent is well configured, and the same input can produce different output at different times. Customer decides what its Agents and the Dashboard Assistant are used for, configures, tests and supervises them, and is responsible for reviewing output before relying on it where the consequences of an error could be significant. Accordingly, Subcontext does not warrant that Agent Output or the Dashboard Assistant's output will be accurate or suitable for any purpose, and is not liable for the content of AI output as such, or for actions an Agent takes within the parameters Customer has configured.

Subcontext remains liable, in accordance with Section 16, for its own breach of this Agreement, including defects in the Service, security failures, and failure to apply the Guardrails, consent checks, approvals and other controls as Customer has configured them and as the Documentation describes.

7. Communications and Messaging

7.1 Channels

The Service lets Agents and Users communicate with Contacts by web chat, email, SMS, WhatsApp and voice calls, where Customer's Plan includes the channel. Each channel depends on a third-party carrier or platform (including Twilio for SMS, voice and phone numbers, Meta for WhatsApp, and Amazon SES for email) and is subject to that provider's rules, approvals and availability.

7.2 Messaging Compliance

Customer is responsible for ensuring that the communications it sends, or its Agents send, through the Service comply with the law, including the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), the ICO's direct marketing guidance, the advertising codes, and the law of any other country where Contacts are located. In particular, Customer is responsible for:

- obtaining a Contact's prior consent before an Agent makes an automated or AI voice call to them for direct marketing, which PECR treats as an automated calling system;
- screening numbers against the Telephone Preference Service and Corporate Telephone Preference Service, and keeping its own do-not-call list, before making live marketing calls;
- presenting a valid calling line identification on marketing calls;
- telling Contacts they are interacting with AI where the law or regulator guidance requires it, including under Article 50 of the EU AI Act for Contacts in the European Union (the Service provides an AI disclosure rule that Customer can apply); and
- for Contacts who are children, having a lawful basis and complying with the ICO's Age Appropriate Design Code where it applies.

The Service's checks, including its Telephone Preference Service check, are safeguards that rely on the information Customer provides; they do not transfer these responsibilities to Subcontext.

7.3 Consent and Lawful Basis

(a) **Lawful basis.** Customer must have a lawful basis for each kind of message it sends to each Contact on each channel and, where the law requires it (for example, for electronic marketing under PECR), the Contact's consent or a valid soft opt-in. Not every message needs consent: messages about a Contact's own enquiry, quote or policy may rely on another lawful basis, such as performance of a contract or legitimate interests, where Customer has determined that basis applies. Establishing and evidencing the lawful basis, and obtaining consent where it is needed, rests with Customer.

(b) **Consent settings.** The Service lets Customer set, for each place it collects a Contact's details or asks them a question, what the Contact is shown, how they are asked, and what their answer permits ("Consent Rules"), and organisation-wide settings for how strictly consent is applied ("Consent Policy"). Customer is responsible for the Consent Rules and Consent Policy it configures, including their wording, their accuracy, and their consistency with Customer's own privacy notice. The Service refuses some settings that fall below minimum legal requirements; those checks are a safeguard only, are not legal advice, and do not mean that a configuration Customer saves is lawful.

(c) **Consent records.** The Service records each decision a Contact makes about being contacted, and each decision Customer records for them: the purpose, the channel, the lawful basis, the wording in force

when it was given, where it was given, and supporting evidence such as the time, IP address and browser ("Consent Records"). Where Customer's Users record a Contact's consent through the Service, they must record how and when it was given. Customer warrants that any consent it records, imports, or receives from a third party (including through the API, an integration or a partner) was validly given and that Customer holds evidence of it.

(d) **How the Service applies them.** Before each message or call, the Service checks the Consent Records against Customer's Consent Policy and does not send a message for which it holds no permitted basis. It honours the opt-outs it receives, including STOP replies, unsubscribe links and replies, the preference page described in paragraph (e), and complaints that an email is spam. These checks rely on the information Customer provides and configures; they reduce, and do not remove, Customer's responsibility under Section 7.2. Subcontext is responsible for applying them as described in this paragraph; Customer is responsible for communications sent in reliance on its Consent Rules, Consent Policy, message purposes or Consent Records, and for communications sent without a lawful basis or consent that Customer was required to establish or obtain.

(e) **Preference page.** The Service gives each Contact a page, linked from Customer's messages, where they can see and change what they have agreed to, and supports one-click unsubscribe from email. Customer must not remove, hide or obstruct these mechanisms.

(f) **Message purposes.** Customer is responsible for the purpose it gives each message, template and automated message (service, marketing, or essential). A message marked essential (for example, policy documents, renewal notices and payment notices) may be sent to a Contact who has objected to other service messages, so Customer must mark a message essential only where it is genuinely necessary.

(g) **Third-party marketing.** Recording consent to marketing on behalf of other companies is available only where Subcontext has enabled it for Customer's Organisation. Subcontext may decide whether to enable it after reviewing how Customer will use it, and may withdraw it.

7.4 Message Content

Customer is responsible for the content of its messages, including content generated by its Agents, and for ensuring that it complies with advertising standards, consumer protection law and the rules of its regulators. Subcontext does not review or approve messages before they are sent. WhatsApp templates and sender profiles are submitted to Meta for approval and may be rejected, restricted or withdrawn by Meta; Subcontext does not control those decisions.

7.5 Phone Numbers

Phone numbers used for SMS, WhatsApp and voice are rented from Subcontext's carrier, Twilio, and are registered in Subcontext's name under the regulatory records the carrier requires. Customer has the use of a number while it is assigned to Customer's Organisation and the rental is paid, and acquires no ownership of it. Numbers are charged monthly as described in Section 12.3. Customer must supply, and keep accurate, any business identity information the carrier or regulator requires for a number, and Subcontext may release a number that cannot be kept compliant after telling Customer why. On Customer's written request made before the Termination Date or before a number is released, Subcontext will cooperate with porting a number out to a provider Customer chooses, where the carrier and the regulatory rules allow it; Customer pays any charges the carriers make for the port. A number that is not ported out is returned to the carrier when it is released or the Subscription ends, and may be reassigned. The Service does not currently port numbers in.

7.6 Voice Calls and Recordings

Voice calls with Agents may be recorded and transcribed where Customer enables recording. Customer is the controller of call recordings and is responsible for: (a) determining whether it may lawfully record and monitor calls; (b) announcing recording to Contacts, using the announcement the Service plays at the start of a call (which Customer can change) or its own; and (c) any regulatory record-keeping obligation that applies to its calls. Recordings and transcripts are kept for the retention period Customer sets in the Organisation's settings and are then deleted, except where they are under a legal hold; a retention period of zero keeps them until Customer deletes them or they are deleted under Section 19.6. Subcontext does not listen to or read recordings except as needed to operate the Service or as permitted by Section 9.6.

7.7 Outreach and Contact Uploads

Where Customer uploads or imports Contact lists for outreach campaigns, nurture sequences or follow-ups, Customer warrants that it holds a lawful basis, and where required the consent, to contact each person by the channel used, that the data is accurate and was obtained lawfully, and that any person who has opted out has been removed. Where Customer confirms through the Service the basis on which people it uploads or adds to an outreach stream may be contacted, that confirmation is kept as a Consent Record under Section 7.3. The Service checks each message against the Consent Records and honours opt-outs it receives (see Section 7.3), and holds or stops messages when the Organisation is out of Credit or its Subscription has lapsed (see Section 12), but it does not verify that the consent or lawful basis Customer records or confirms for an upload was validly obtained.

7.8 Custom Domains and Hosted Sites

Customer may connect its own domains to the Service for sending email and for hosting pages and forms. Customer is responsible for the DNS records the Service asks it to create and for keeping them in place; a domain that fails verification, or whose records are removed, stops sending or serving until it is corrected. Content on hosted pages and forms is Customer Content and must comply with the AUP.

7.9 Advertising Conversion Reporting

Where Customer connects a Google or Meta advertising account to an Organisation, the Service reports conversion events to that platform on Customer's instructions. Where Customer turns on enhanced matching, the Service also sends Contacts' email addresses and phone numbers, hashed before they leave the Service. Customer is responsible for having a lawful basis, and any consent PECR requires, for that reporting, for describing it in its privacy information, and for complying with the advertising platform's terms, including Google's policies for enhanced conversions and Meta's Business Tools Terms. The Service does not report conversions to an advertising platform unless Customer connects one.

8. Payments and Insurance Journeys

8.1 Payment Processing

The Service can collect payments from Contacts through Stripe, by card or by Bacs Direct Debit. Card details are entered into Stripe's payment forms and are never stored by Subcontext. Where a Contact pays by Direct Debit, the Service collects the bank details needed to set up the mandate, stores them encrypted, and passes them to Stripe. Payment processing is performed by Stripe under Stripe's own terms. Subcontext is not a payment institution and does not hold Customer's or Contacts' funds.

8.2 Customer's Responsibilities for Payments

Customer is responsible for: the amounts it charges and the products and services it charges for; refunds, chargebacks and disputes with its Contacts; its own compliance with the Payment Card Industry Data Security Standard to the extent it applies to Customer; the Direct Debit Guarantee obligations that attach to mandates collected in its name; and payments initiated by its Agents within the parameters it has configured. Where Customer enables Agents to take payments, Customer must configure appropriate amount limits and approvals, tell Contacts that an AI Agent may take their payment, and comply with consumer protection law, the Payment Services Regulations 2017 and the rules of its regulators that apply to it.

8.3 Insurance Journeys and Connected Accounts

Where Customer's Plan includes the insurance engine, the Service can run quote, application, binding, premium collection, policy administration and claims journeys for Customer's own products. Premiums are collected into a Stripe account connected to Customer's Organisation (a Stripe Connect account in Customer's name), by card or by Direct Debit mandate, under Stripe's connected account agreement, and Subcontext is not a party to the payment and does not hold the funds. Customer is the insurer, intermediary or other regulated party for every policy the Service handles, and is responsible for the products, their terms, their pricing and the regulatory permissions they require. Subcontext is not an insurer, does not give advice, and does not arrange, bind or administer insurance on its own account.

8.4 Platform Fee on Premiums

Where Customer collects premiums through a connected account, Subcontext charges a platform fee on each premium collected, at the rate agreed in an Order Form or, if there is none, the rate Subcontext notifies to Customer before Customer first collects premiums. Stripe deducts the platform fee from the premium as an application fee when the premium is collected. A change to the rate is a change to Fees under Section 12.12.

9. Customer Data and Data Protection

9.1 Ownership and Licence

As between the parties, Customer owns Customer Data. Customer grants Subcontext a non-exclusive, royalty-free licence, for the duration of this Agreement and the periods in Section 19.6, to host, store, copy, process, transmit and display Customer Data only to the extent needed to provide, support and secure the Service for Customer, to comply with law, and as otherwise instructed by Customer. Subcontext's use of personal data within Customer Data is further limited by the DPA.

9.2 Roles of the Parties

For personal data in Customer Data, Customer is the controller and Subcontext processes it as Customer's processor under the DPA. Subcontext is an independent controller only of the personal data it collects for its own purposes, as described in section 2.3 of the DPA and in the Privacy Policy, such as Users' account details, billing records, platform security data and the records of acceptance of these Terms.

9.3 Data Processing Agreement

The DPA forms part of this Agreement and sets out the terms required by Article 28 of the UK GDPR, including instructions, confidentiality, security, sub-processors, international transfers, assistance with data subject requests, breach notification, deletion and return, and audit. The canonical list of sub-processors is in section 6.1 of the DPA.

9.4 Customer's Data Protection Obligations

Customer is responsible, as controller, for:

- having a lawful basis for the processing it carries out through the Service, including collection, storage, profiling (including vulnerability detection), automated decision-making and communications;
- giving Contacts the privacy information the law requires. Customer's privacy information must cover the processing carried out through the Service, including AI-assisted interactions and the categories of recipients involved; Customer may do this by linking to the Subcontext Consumer Notice, which Subcontext keeps up to date;
- responding to data subject requests, which the Service's erasure and data rights tools help with;
- applying appropriate retention periods to Contact data, using the retention settings and deletion tools the Service provides, and deleting data it no longer needs; and
- for Contacts who are children (for example where an insurance product covers a child as an insured life), having a lawful basis and complying with the ICO's Age Appropriate Design Code where it applies.

9.5 Usage Data and No Training

Subcontext may collect and use operational metrics about the use of the Service, such as volumes, latency, costs and errors ("Usage Data"), to operate, secure, support, bill for and improve the Service. Usage Data does not identify any User or Contact, and Subcontext does not disclose Usage Data that identifies Customer to anyone else. Subcontext does not use Customer Data, or personal data of Contacts, whether or not anonymised, to train or fine-tune any AI model.

9.6 Support Access

Subcontext's platform administrators can open an Organisation's dashboard as one of its Users ("impersonation") to investigate a problem, provide support, or respond to a security incident. Impersonation is limited to those purposes, is recorded in the audit log with who did it, when, and every action taken, and is never used to send messages, take actions or make purchases on Customer's behalf unless Customer has asked for that in writing.

9.7 Audit Log, Compliance Decision Trail and Compliance Check Runs

The Service keeps an audit log of significant actions taken in an Organisation (by Users, Agents and Subcontext), which Customer can review in the dashboard and which is kept for two (2) years. It also keeps a tamper-evident compliance decision trail of Guardrail, Agent Policy and consent decisions, kept for the retention period Customer configures (six (6) years by default). Where Customer runs compliance checks against an Agent, the Service creates test conversations and synthetic records for that purpose; those runs are Customer Data, are kept as evidence of the check, and their synthetic supporting records are deleted after a limited period.

9.8 Connected Google Services

Customer may connect Google Calendar and Google Sheets to an Organisation for appointment scheduling and record export. For data obtained from Google Calendar and Google Sheets, the Service requests only the Google permissions those features need, uses the data only to provide those features, does not use it for advertising, and does not transfer it to anyone else except as needed to provide those features or as required by law, in accordance with the Google API Services User Data Policy, including its Limited Use requirements. The Privacy Policy describes the data involved. Customer can disconnect a Google account at any time from the Organisation's integration settings, which stops further access. Advertising conversion reporting under Section 7.9 is separate and does not use data obtained from Google Calendar or Google Sheets.

9.9 Context Blocks

Customer is responsible for the content of its Context Blocks, including documents and files it uploads, and warrants that it has the right to use them and make them available to its Agents.

10. Security and Incidents

10.1 Subcontext's Security Obligations

Subcontext will implement and maintain appropriate technical and organisational measures to protect the Service and Customer Data against unauthorised or unlawful processing and against accidental loss, destruction or damage. These include: encryption of the whole database at rest and field-level encryption of sensitive values such as integration credentials and Direct Debit bank details; TLS 1.2 or higher in transit; a web application firewall and rate limits; role-based access with data isolated by Organisation; two-factor authentication, enforced by default for new Organisations; an immutable audit log; signature-verified webhooks; vulnerability scanning; regular security assessments of the platform infrastructure; documented incident response procedures; and logging and alerting. The measures are described in the DPA and in the security policies published at /trust. Subcontext will keep its measures under review and will not materially reduce the overall level of protection they provide during the term of this Agreement.

10.2 Security Incidents and Breach Notification

Subcontext will notify Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach, or any other security incident, affecting Customer Data. Subcontext may provide information in phases as it becomes available, will cooperate with Customer's investigation and remediation, and keeps records of incidents. The DPA sets out the detail for Personal Data Breaches.

10.3 Customer's Security Obligations

Customer is responsible for the security of its Users' credentials, API keys and tokens, for the devices its Users use to access the Service, and for its own systems connected to the Service. Customer must report suspected security incidents affecting the Service to hello@subcontext.com without undue delay.

10.4 Backups and Recovery

Subcontext takes automated database backups that allow point-in-time recovery for seven (7) days. Subcontext's business continuity arrangements are described at /trust/business-continuity-disaster-recovery and, for Regulated Customers, in Schedule 1.

11. Intellectual Property

11.1 Subcontext's Intellectual Property

Subcontext and its licensors own all intellectual property rights in the Service, including its software, interfaces, designs, Documentation, APIs and trade marks. Subject to this Agreement and payment of the Fees, Subcontext grants Customer a non-exclusive, non-transferable right, for the term of its Subscriptions, to use the Service, and to permit its Users to use it, for Customer's internal business purposes. No other rights are granted.

11.2 Agent Output

Subcontext does not claim ownership of Agent Output, and as between the parties any rights in Agent Output belong to Customer. Agent Output is generated by third-party AI models from Customer's configuration and data; Subcontext does not warrant that it is original or protectable, and Customer is responsible for ensuring that its use of Agent Output does not infringe third-party rights. Section 15.2 covers claims about the Service itself.

11.3 Feedback

If Customer gives Subcontext feedback or suggestions about the Service, Subcontext may use them without restriction or obligation, provided that Subcontext does not disclose Customer's Confidential Information or identify Customer as their source.

12. Fees, Subscriptions and Payment

12.1 Fees and VAT

Customer will pay the Fees for its Plan, as published in the Service when it subscribes or changes Plan, or as set out in an Order Form. Fees are in pounds sterling unless otherwise stated and are exclusive of VAT, which is charged at the prevailing UK rate where it applies, except that where Customer is established outside the UK and has supplied a valid VAT registration number, VAT is accounted for under the reverse charge or as otherwise required by law. Plan descriptions and comparisons published on the Service are summaries and are subject to this Agreement, including the fair use provisions of Section 12.13.

12.2 Usage-Based Charges

Certain charges are usage-based: AI model usage, messages sent and received (SMS, WhatsApp and email, with inbound email measured by size), voice call minutes and phone number rental. Each use is priced at Subcontext's rate card in effect when it happens (Section 12.3) and is recorded against the Organisation in pounds sterling at that moment; the usage page shows every use and what it cost. Charges are incurred on actual usage, including usage generated by autonomous Agent activity.

Usage-based charges are settled in one of two ways, and the Billing page shows which applies to an Organisation:

- **By Credit** (the default for new Organisations): each charge is drawn from the Organisation's Credit as it is incurred, as described in Section 12.16.
- **In arrears**: each calendar month (UTC) the Plan includes a usage allowance for AI usage and a separate allowance for messaging and calls. Usage beyond an allowance in a month is added, with

VAT, to the Organisation's next invoice; for invoiced accounts it is invoiced separately. Usage within the allowance is not charged, and unused allowance does not carry forward.

The allowances and Credit that apply to each Plan are those described on the Service at the time of purchase or in an Order Form.

12.3 Third-Party Costs and the Rate Card

Usage-based charges are priced at Subcontext's rate card, which is the cost Subcontext pays its providers (for AI models, messaging, calls and phone numbers) plus Subcontext's margin, converted to pounds sterling under Section 12.19. Where a provider changes its prices, or the exchange rate Subcontext sets under Section 12.19 changes, the corresponding rates may change with immediate effect for use after the change. Subcontext will give Customer at least thirty (30) days' notice of an increase in its margin. Phone number rental is charged monthly for each number assigned to the Organisation at the time of the monthly charge, for the whole month: a number taken on during a month is charged in full for that month and a number released during a month is not refunded for it.

12.4 Late Payment

If Customer does not pay any amount when due, Subcontext may charge interest on it at four per cent (4%) a year above the Bank of England base rate, accruing daily from the due date until payment, and may restrict access under Section 12.11 or suspend under Section 18.

12.5 Refunds

Fees are not refundable, and unused Included Credit, unused usage allowances and unused parts of a Billing Period do not carry forward or give rise to a refund, except that:

- (a) unused Bought Credit is refundable on request as set out in Section 12.16;
- (b) where Customer terminates a Subscription under Section 14.3 (warranty), Section 19.3 (Subcontext's material breach or insolvency), Section 21.2 (materially adverse change), Schedule 1 (regulator direction), or after objecting to a new sub-processor under the DPA, or where Subcontext terminates under Section 13.3 (force majeure), Section 15.5 (infringement) or Section 19.4 (convenience), Subcontext will refund the prepaid Fees for the period after the Termination Date, pro rata, and all unused Bought Credit, and no subscription Fees are payable for any part of a Fixed Term after the Termination Date;
- (c) Subcontext may, at its discretion, issue refunds or add Credit in individual cases, which does not create an entitlement in other cases; Credit added by Subcontext is treated as Bought Credit, and every adjustment is shown with its reason in the Organisation's credit history; and
- (d) refunds required by law are not affected.

12.6 No Set-Off

Customer will pay all amounts due without set-off, counterclaim, deduction or withholding, other than any deduction of tax required by law.

12.7 Usage Limits and Cost Protection

Each Plan includes default usage allowances, including daily AI spend limits, that Subcontext applies technically; Customer may ask for them to be adjusted. Daily AI spend limits are separate from Credit and from the monthly allowances: when a daily limit is reached, AI activity pauses until the next day (UTC)

whatever Credit or allowance remains. Subcontext will use reasonable efforts to alert Customer to abnormal cost patterns, and may throttle or pause activity that significantly exceeds the Organisation's normal usage to protect Customer and the Service, telling Customer when it does. These controls are safeguards: Customer remains responsible for monitoring its usage through the usage page and is liable for charges incurred before any pause. A pause under this Section is not a suspension under Section 18.

12.8 Subscriptions and Automatic Renewal

Subscriptions renew automatically at the end of each Billing Period until cancelled, except a Subscription with a Fixed Term, which follows Section 12.21. By providing a payment method, Customer authorises Subcontext (through its payment processor, Stripe) to charge that payment method the recurring subscription Fee for the selected Plan, applicable taxes and any usage-based charges, at the start of each Billing Period and at the other times described in these Terms (including prorated charges on upgrade, top-ups Customer buys, and automatic top-ups where Customer has enabled them under Section 12.17). Customer is responsible for keeping a valid payment method on file.

12.9 Cancellation

Customer may cancel a Subscription at any time through the Billing page of the Service or by contacting Subcontext. Cancellation takes effect at the end of the current Billing Period: access to paid features continues until that date, no further renewal Fees are charged, and no pro rata refund is given for the remainder of the period except as set out in Section 12.5. If the Subscription is past due when it is cancelled, access ends at the end of the grace period described in Section 12.11 if that comes first. A cancellation may be reversed through the Billing page at any time before it takes effect. On cancellation Subcontext will tell Customer how much Bought Credit remains, which stays usable until access ends and is refundable as set out in Section 12.16. A Subscription with a Fixed Term cannot be cancelled through the Billing page and ends only as set out in Section 12.21.

12.10 Plan Changes

- **Upgrades** take effect once the prorated charge for the upgrade is paid. Customer is charged a prorated amount reflecting the unused portion of the current Billing Period; until that charge is paid the current Plan and its allowances continue, and if it is not paid within the time the payment processor allows (currently about one day) the upgrade lapses and may be requested again. When the upgrade takes effect the Billing Period resets from that date and, for an Organisation billed by Credit, the new Plan's Included Credit becomes available for the rest of the calendar month, less any Included Credit already used that month.
- **Downgrades** take effect at the start of the next Billing Period, when the new Plan's allowances and Included Credit apply. A scheduled downgrade may be cancelled through the Billing page at any time before it takes effect.
- The price Customer pays for a Plan is the price agreed when Customer subscribed to it or changed to it, and is not affected by a later change to the published price except as set out in Section 12.12.
- On a downgrade, or on lapse of a Subscription, features, integrations, channels and usage allowances of the higher Plan may become inactive, and resources exceeding the lower Plan's allowances may be restricted. Subcontext keeps the associated Customer Data in accordance with Section 19.6 and the retention settings of the Organisation.

12.11 Failed Payments and Grace Period

If a renewal or other subscription charge fails, Subcontext (through Stripe) may retry the payment and will notify Customer. Customer's access to paid features continues for a grace period (currently fourteen (14) days) from the first failed charge, during which Customer may update its payment method through the Billing page. Subcontext will remind Customer before the grace period ends. Adding a new card during the grace period retries the outstanding charge on it immediately. If payment is not collected by the end of the grace period, access to the Service is restricted until payment is made: the dashboard directs Customer to the Billing page, and Agents, voice calls, outreach campaigns and outbound messages pause. If payment remains outstanding, Subcontext may terminate the Subscription under Section 19.3. Customer remains liable for all Fees accrued up to the Termination Date.

12.12 Changes to Fees and Plans

Subcontext may change subscription Fees, its margin on usage-based charges, the platform fee on premiums, and the composition of Plans (including features and usage allowances). A change that increases the Fees or materially reduces the features of Customer's current paid Plan will be notified to Customer at least thirty (30) days in advance by email and in the dashboard, and takes effect from Customer's next Billing Period after the notice period ends. If Customer does not accept the change, it may cancel the Subscription under Section 12.9 before the change takes effect. During a Fixed Term, changes under this Section apply only as set out in Section 12.21. Changes to rates driven by provider prices or exchange rates follow Section 12.3. Where a price has been individually agreed in an Order Form, it changes only as the Order Form provides or as both parties agree in writing.

12.13 Usage Allowances and Fair Use

Each Plan includes the usage allowances described on the Service at the time of purchase (for example, limits on the number of Agents, Users, active outreach campaigns and monthly nurture messages). Subcontext may enforce these allowances technically, and exceeding an allowance may require an upgrade to a higher Plan. Where a Plan describes any allowance as "unlimited", that allowance is subject to fair use: Subcontext may apply reasonable technical ceilings consistent with normal business use of the relevant feature and will not treat ordinary business usage as exceeding fair use.

12.14 Invoiced Accounts

Where agreed in an Order Form (including for Enterprise plans), Fees may be invoiced rather than collected by card. Subscription Fees for invoiced accounts are invoiced monthly in arrears: each month of the Plan, counted from the date it was activated, is invoiced once that month has ended, with VAT (unless the reverse charge applies), and usage beyond the Plan's allowances is invoiced separately. Where a fixed term ends part-way through a month, that month is invoiced in full when the term ends. Invoices are due by the date stated on them, which is thirty (30) days after the end of the month invoiced (or, for the final month of a fixed term, after the end of the term) unless the Order Form says otherwise. An invoice that remains unpaid after its due date starts the grace period described in Section 12.11, with the same consequences. Where a Fixed Term has been agreed, Section 12.21 applies.

12.15 Free Trials

Subcontext may offer free trial workspaces, including trial workspaces created through partner-embedded features (such as Nurture with AI). Trial workspaces carry limited features and usage allowances, are not covered by the warranty remedy in Section 14.3 or any service level, and may be changed, suspended or

withdrawn by Subcontext at any time. Continued use of a trial workspace's full features requires selecting and paying for a Plan. A trial workspace that has not been converted to a paid Plan is deleted, together with the Contact details and conversations in it, once no nurture or other outreach has been started from it for ninety (90) days. Where Subcontext holds an email address for a User of the trial workspace, it will send a reminder before the deletion.

12.16 Prepaid Credit

Where an Organisation is billed for usage by Credit:

- **Included Credit.** The Plan's Included Credit is added to the Organisation's balance on the first day of each calendar month (UTC). It is used before Bought Credit, does not carry forward, and whatever remains of it at the end of the month expires.
- **Bought Credit.** Customer may buy Credit through the Billing page in the fixed amounts offered there (currently from £10 to £1,000). Each purchase is charged immediately, with VAT, to the card Customer chooses and invoiced. Credit is added when the payment is confirmed. Bought Credit does not expire while the Subscription is live and carries forward from month to month.
- **Drawing down.** Each usage-based charge is drawn from the balance as it is incurred. Because a charge is priced when the use completes, a charge can occasionally land that the remaining balance does not fully cover; Subcontext absorbs any such shortfall and it is not carried into the next month.
- **Running out.** Subcontext will notify the Organisation's owners and managers when Credit falls below ten per cent (10%) of the month's total (Included Credit plus Bought Credit added that month) and again when it is exhausted. When Credit is exhausted, Agents, voice calls, outreach campaigns and outbound messages pause until Credit is added or the next month's Included Credit arrives. Messages required by law (for example an unsubscribe confirmation) are still sent. Outreach messages held for lack of Credit resume automatically when Credit is added, and are abandoned if Credit is not added within thirty (30) days. A pause for lack of Credit is not a suspension under Section 18.
- **Statement.** Every movement on the balance is recorded, and Customer can view its credit history and download a monthly statement from the Billing page.
- **Reserved Credit.** While an Agent conversation or voice call is in progress, a small amount of Credit is reserved for it and released when the interaction ends, so the available balance can briefly be lower than the balance shown in the credit history.
- **Reversed purchases.** If a purchase of Credit is refunded, charged back or otherwise reversed, the Credit it bought is removed from the balance, and if it has already been used the shortfall is payable by Customer. A chargeback against Fees properly charged is treated as non-payment.
- **Refund of Bought Credit.** Included Credit is never refundable. When a Subscription is cancelled or ends, Customer may ask, within ninety (90) days of the Termination Date, for a refund of any Bought Credit that remains unused; Subcontext will refund it to the card it was bought with (or, if that is not possible, to an account Customer nominates) and issue a credit note, and the refunded amount is removed from the balance. Bought Credit that has been used is not refundable.

12.17 Automatic Top-Ups

Customer may enable automatic top-ups on the Billing page. Where enabled, Customer authorises Subcontext (through Stripe) to charge the top-up amount Customer has chosen to the Organisation's default card whenever Credit falls below ten per cent (10%) of the month's total, subject to the monthly limit on automatic top-ups that Customer sets on the Billing page (which Subcontext applies with a default

of £500). Subcontext will not charge an automatic top-up more than once within an hour of any other Credit purchase, and will notify the Organisation's owners if an automatic top-up cannot be taken or the monthly limit has been reached. Automatic top-ups stop when Customer disables them, when the monthly limit is reached, or when the Organisation has no card on file. Each automatic top-up is charged and invoiced like any other purchase of Credit.

12.18 No-Charge Plans

Subcontext may, at its discretion, provide an Organisation with a Plan at no subscription charge. Usage-based charges continue to apply as described in this Section 12, unless Subcontext has agreed otherwise in writing; the Included Credit or allowances for a no-charge Plan are those agreed for it, which may be nil. Subcontext may end a no-charge Plan by giving Customer at least fourteen (14) days' notice, after which a paid Plan is required to keep access to the Service. Credit already on the Organisation's balance is unaffected by the end of a no-charge Plan.

12.19 Currency Conversion

Subcontext buys AI model usage and telephony from its providers in US dollars and prices them to Customer in pounds sterling. Each use is converted at the exchange rate Subcontext has set at that time, which Subcontext reviews and updates periodically rather than at a live market rate; the rate applied is recorded with each use and does not change afterwards. The sterling price of a use therefore reflects exchange rate movements as well as provider price changes.

12.20 Billing Disputes

Customer must raise any query about a charge, an invoice, a credit note or an entry in its credit history within thirty (30) days of the date of the invoice or statement concerned, or of the entry appearing in the credit history, giving reasons. Subcontext will investigate promptly and correct any error it finds. Undisputed amounts remain payable on time, and a charge not queried within that period is accepted as correct except where Subcontext's own records show an error.

12.21 Fixed Terms

Where an Order Form sets a Fixed Term, this Section applies to that Subscription, and the Order Form prevails where it says something different.

- (a) **Commitment.** Customer commits to the Subscription for the whole Fixed Term. The subscription Fees for every month of the Fixed Term are payable even if Customer stops using the Service, reduces its usage or asks to close its Organisation before the Fixed Term ends, and continue to be invoiced as they fall due under Section 12.14. If Subcontext terminates under Section 19.3 because of Customer's breach or insolvency, the subscription Fees for the rest of the Fixed Term become payable immediately.
- (b) **Early termination by Customer.** Customer may not end the Subscription for convenience during the Fixed Term. Customer may end it early under Section 14.3 (warranty), Section 19.3 (Subcontext's material breach or insolvency), Section 21.2 (materially adverse change), Schedule 1 (regulator direction), or after objecting to a new sub-processor under the DPA; in each of those cases, and where Subcontext ends it under Section 13.3, Section 15.5 or Section 19.4, no subscription Fees are payable for the rest of the Fixed Term, and Customer pays only for the Service provided up to the Termination Date.

- (c) **Prices and Plan during the Fixed Term.** The Fees, allowances and features agreed in the Order Form apply for the whole Fixed Term. Changes under Section 12.12 to subscription Fees, Subcontext's margin, the platform fee on premiums or the Plan's allowances and features do not apply until the Fixed Term ends, except where they benefit Customer. Changes to Third-Party Costs under Section 12.3 continue to apply, unless the Order Form fixes those rates.
- (d) **Changes of Plan.** Customer may move to a higher Plan during the Fixed Term by agreement in writing. A move to a lower Plan, or a reduction in committed volumes, takes effect only at the end of the Fixed Term unless both parties agree otherwise in writing.
- (e) **End of the Fixed Term.** Unless the Order Form provides for renewal or the parties agree a renewal in writing, the Subscription ends at the end of the Fixed Term. Access to the paid features of that Plan continues to the end of the Fixed Term, after which Customer may choose a published Plan to continue using the Service. Subcontext will contact Customer before the Fixed Term ends to discuss renewal, but the Subscription ends on that date whether or not it does. Where an Order Form provides for automatic renewal, either party may stop the renewal by written notice given at least the period before the end of the Fixed Term that the Order Form states or, if it states none, at least sixty (60) days before.
- (f) **Notices.** Notices about a Subscription with a Fixed Term are given under Section 23.5, not through the Billing page.

13. Availability, Support and Force Majeure

13.1 Availability and Maintenance

Subcontext will use reasonable efforts to keep the Service available. Subcontext may carry out scheduled and emergency maintenance, which may interrupt the Service; it will try to schedule planned maintenance outside UK business hours and to give advance notice of it, and will keep emergency maintenance to what is necessary. A service level agreement with availability commitments and service credits applies only where an Order Form includes one.

13.2 Support

Support is available by email to support@subcontext.com and through support tickets in the Service, Monday to Friday, 09:00 to 17:30 UK time, excluding English public holidays. Subcontext aims to give a first response within four (4) business hours on Enterprise plans, one (1) business day on Professional plans and two (2) business days on other Plans. These are targets, not guaranteed service levels unless an Order Form says so. The current support terms are published at /trust/service-levels-support.

13.3 Force Majeure

Neither party is liable for a failure or delay in performing its obligations caused by events beyond its reasonable control ("Force Majeure Event"), such as natural disasters, pandemics, war, terrorism, civil unrest, government action, failure of the public power or telecommunications networks, or a cyberattack that the affected party's compliance with its security obligations could not reasonably have prevented. A failure of a party's own subcontractors or suppliers (including Subcontext's hosting, AI and messaging providers) is a Force Majeure Event only if the subcontractor or supplier is itself prevented by an event that would be a Force Majeure Event and the party could not reasonably have used an alternative. A Force Majeure Event does not excuse an obligation to pay money.

The affected party must notify the other as soon as reasonably practicable, with the expected duration, and use reasonable efforts to mitigate the effects. If a Force Majeure Event prevents performance of a material part of this Agreement for more than thirty (30) consecutive days, either party may terminate the affected Subscription by written notice, with a refund under Section 12.5.

14. Warranties

14.1 Mutual Warranties

Each party warrants that it is validly incorporated or established, and has the power and authority to enter into and perform this Agreement.

14.2 Service Warranty

Subcontext warrants that the Service will be provided with reasonable skill and care and will perform materially in accordance with the Documentation. This warranty does not apply to a failure caused by Customer Content, Customer's configuration or instructions, use of the Service other than in accordance with this Agreement and the Documentation, third-party services that Customer chooses to connect, Beta Features, or trial workspaces (which are provided with reasonable skill and care but without the remedy in Section 14.3). The content of AI output is governed by Section 6.7.

14.3 Remedy

If the Service does not comply with Section 14.2, Customer must notify Subcontext with reasonable details, and Subcontext will use reasonable efforts to correct the non-conformity promptly or provide a workaround. If Subcontext does not do so within thirty (30) days of the notice, either party may terminate the affected Subscription by written notice, and Subcontext will refund prepaid Fees and unused Bought Credit under Section 12.5. This remedy does not limit Customer's right to claim damages for breach of Section 14.2, subject to Section 16.

14.4 Exclusion of Other Terms

Subcontext does not warrant that the Service will be uninterrupted or error-free. Except as expressly set out in this Agreement, all warranties, conditions and other terms implied by statute or common law are excluded to the fullest extent permitted by law.

14.5 Customer Warranties

Customer warrants that: it holds, and will maintain, every authorisation, permission and registration needed for the activities it carries out using the Service; its declaration of regulated status under Section 5.2 is accurate; it has the rights, lawful bases and consents needed to provide Customer Data to Subcontext and to have it processed under this Agreement; and its use of the Service, and Customer Content, will comply with the law and the AUP.

15. Indemnities

15.1 Customer's Indemnity

Customer will indemnify Subcontext against all losses, damages, costs (including reasonable legal fees) and liabilities arising from a third-party claim, including a claim by a Contact or a regulator, to the extent it

arises from:

- (a) Customer's breach of this Agreement, the AUP or the law;
- (b) Customer Content;
- (c) Customer's configuration of the Service and its instructions, including its Agents, Tools, Consent Rules, Consent Policy, message purposes and payment flows; or
- (d) Customer's lack of a lawful basis, consent or other authorisation it was required to have,

except to the extent the claim is caused by Subcontext's breach of this Agreement or negligence.

15.2 Subcontext's Intellectual Property Indemnity

Subcontext will defend Customer against any third-party claim that Customer's use of the Service in accordance with this Agreement infringes that third party's intellectual property rights enforceable in the United Kingdom (including patents, copyright, database rights, design rights and trade marks) ("IP Claim"), and will indemnify Customer against damages and costs finally awarded against Customer, or agreed by Subcontext in settlement, in respect of the IP Claim.

15.3 Subcontext's Data Protection Indemnity

Subcontext will indemnify Customer against all losses, damages, costs (including reasonable legal fees), and fines and penalties to the extent the law allows them to be indemnified, arising from a third-party or regulatory claim to the extent it arises from Subcontext's breach of the DPA or of data protection law in providing the Service.

15.4 Conduct of Claims

The indemnities in this Section 15 are conditional on the indemnified party: (a) notifying the indemnifying party in writing promptly after becoming aware of the claim (a delay relieves the indemnifying party only to the extent it is prejudiced by it); (b) allowing the indemnifying party to control the defence and settlement of the claim, provided that the indemnifying party will not agree a settlement that requires an admission of fault by, or imposes an obligation on, the indemnified party without its consent (not to be unreasonably withheld); (c) giving reasonable cooperation at the indemnifying party's cost; (d) not making any admission about the claim without the indemnifying party's consent; and (e) taking reasonable steps to mitigate its losses. A regulator's investigation of a Regulated Customer remains under the Regulated Customer's control, and Subcontext will cooperate with it.

15.5 Infringement Remedies

If the Service becomes, or in Subcontext's reasonable opinion is likely to become, the subject of an IP Claim, Subcontext may at its option and expense: (a) obtain the right for Customer to continue using the Service; (b) modify or replace the affected part so that it is non-infringing without material loss of functionality; or (c) if neither is commercially reasonable, terminate the affected Subscription on written notice and refund prepaid Fees and unused Bought Credit under Section 12.5.

15.6 Exclusions from the Intellectual Property Indemnity

Subcontext has no obligation under Section 15.2 to the extent the IP Claim arises from: (a) Customer Content or Customer Data; (b) Agent Output, to the extent the claim arises from the content of the output rather than from the Service itself; (c) a modification of the Service not made by or for Subcontext; (d) combination of the Service with products, services or data not provided or specified by Subcontext, where

the claim would not have arisen without the combination; (e) Customer's continued use of an allegedly infringing part after Subcontext has offered a non-infringing alternative under Section 15.5; or (f) use of the Service in breach of this Agreement.

15.7 Exclusive Remedy for IP Claims

Sections 15.2 and 15.4 to 15.6 state Subcontext's entire liability, and Customer's exclusive remedy, for IP Claims.

16. Limitation of Liability

16.1 Liability That Is Not Limited

Nothing in this Agreement limits or excludes either party's liability for: (a) death or personal injury caused by its negligence; (b) fraud or fraudulent misrepresentation; or (c) any other liability that cannot be limited or excluded by law. This Section 16.1 applies throughout this Agreement and overrides every other provision.

16.2 Excluded Losses

Neither party is liable to the other, whether in contract, tort (including negligence), breach of statutory duty or otherwise, for: (a) loss of profits, revenue or anticipated savings; (b) loss of business, contracts or opportunity; (c) loss of goodwill or damage to reputation; or (d) any indirect or consequential loss, in each case arising under or in connection with this Agreement. This Section 16.2 does not exclude: Customer's obligation to pay the Fees; liability under the indemnities in Section 15; or, where caused by Subcontext's breach of this Agreement, the reasonable costs of restoring or reconstructing Customer Data and of investigating, notifying and remediating a Personal Data Breach.

16.3 Subcontext's General Cap

Subject to Sections 16.1 and 16.4, Subcontext's total aggregate liability arising under or in connection with this Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is limited to the greater of: (a) the Fees paid or payable by Customer in the twelve (12) months before the first event giving rise to liability; and (b) £25,000.

16.4 Subcontext's Data Protection Cap

Subcontext's total aggregate liability arising from its breach of the DPA, data protection law, Section 20 (Confidentiality) or Section 10 (Security and Incidents), and under the indemnities in Sections 15.2 and 15.3, is limited to the greater of: (a) three (3) times the amount of the general cap in Section 16.3; and (b) £250,000. This cap is separate from, and in addition to, the cap in Section 16.3, and amounts paid under it do not reduce that cap.

16.5 Customer's Caps

Subject to Section 16.1:

- (a) **General cap.** Customer's total aggregate liability arising under or in connection with this Agreement is limited to the amount in Section 16.3, except as set out in paragraphs (b) and (c).
- (b) **Indemnity cap.** Customer's total aggregate liability under the indemnity in Section 15.1 is limited to the amount in Section 16.4. This cap is separate from, and in addition to, the cap in paragraph (a), and

amounts paid under it do not reduce that cap.

- (c) **Not limited.** The caps in paragraphs (a) and (b) do not apply to: Customer's obligation to pay the Fees, interest and other amounts due under this Agreement; or Customer's liability arising from its wilful misconduct, or from its deliberate or reckless breach of the AUP or of the law on direct marketing or data protection (for example, knowingly recording consent that was never given, or using the Service to send marketing to people it knows have objected).

16.6 How the Caps Apply

The caps apply to all claims taken together, however many there are, and not per claim or per event.

16.7 Allocation of Risk

The Fees reflect the allocation of risk in this Agreement. Customer may ask for different terms, which may be reflected in different pricing in an Order Form.

16.8 Insurance

Subcontext does not provide insurance cover to Customer, and the Service is not a substitute for Customer's own professional indemnity, cyber or other insurance appropriate to its business.

17. Acceptable Use

Customer must comply, and ensure its Users comply, with the AUP, which forms part of this Agreement and sets out the permitted and prohibited uses of the Service. Without limiting the AUP, Customer must not use the Service to: send spam or unlawful communications; engage in fraud, phishing or deceptive practices; impersonate any person or organisation; generate or distribute illegal or harmful content; circumvent Guardrails, safety features or security measures; access data belonging to other customers; reverse engineer, decompile or disassemble the Service, except to the extent the law permits despite this restriction; or build a competing product or service. A serious or repeated breach of the AUP is a material breach of this Agreement.

18. Suspension

18.1 When Subcontext May Suspend

Subcontext may suspend or restrict Customer's access to all or part of the Service only to the extent reasonably necessary, and only where:

- (a) Customer has committed a material breach of this Agreement (including of the AUP) and has not remedied it within the period stated in Subcontext's written notice, which will be reasonable in the circumstances;
- (b) an amount due remains unpaid after the grace period in Section 12.11, or Customer has charged back Fees properly charged; or
- (c) suspension is needed immediately to address a risk to the security or integrity of the Service or other customers' data, to comply with the law, a court order or a regulator's or carrier's requirement, or to prevent harm to Contacts or third parties.

18.2 Scope and Notice

Subcontext will limit a suspension to what is reasonably necessary (for example a single Agent, channel, phone number or User, rather than the whole Organisation, where that addresses the issue). For suspension under Section 18.1(c), Subcontext will notify Customer, with its reasons, as soon as practicable and where possible before the suspension takes effect. Subcontext will lift a suspension promptly once the reason for it has been resolved. Customer may ask for a suspension to be reviewed by contacting hello@subcontext.com.

18.3 No Deletion as Enforcement

Subcontext will not delete Customer Data as a sanction for breach. During a suspension Customer Data is kept, and after termination it is handled under Section 19.6.

18.4 Other Pauses

Pauses because Credit is exhausted (Section 12.16), a daily AI spend limit is reached or abnormal usage is throttled (Section 12.7), or access is restricted during non-payment (Section 12.11) operate as described in those Sections.

19. Term, Termination and Data on Exit

19.1 Term

This Agreement starts when Customer accepts it and continues while Customer has an Organisation, Subscription or trial workspace in the Service, unless terminated earlier under this Agreement.

19.2 Termination by Customer

Customer may end a Subscription by cancelling it under Section 12.9 (or, for a Subscription with a Fixed Term, as Section 12.21 allows), and may end this Agreement by cancelling all its Subscriptions and asking Subcontext to close its Organisations. Any User may delete their own Account at any time from their profile in the Service or from any App (Account, then Delete account), after confirming their password, or by contacting Subcontext. Deleting an Account signs it out everywhere, removes it from every Organisation and erases the personal details that identify the User; records the Service must keep, such as messages sent on an Organisation's behalf, actions taken, audit logs and acceptances of these Terms, are retained and attributed to a deleted user. Deleting an Account does not cancel any Organisation's Subscription, and an Organisation left without an owner remains Customer's responsibility.

19.3 Termination by Either Party

Either party may terminate this Agreement, or the affected Subscription, with immediate effect by written notice if the other party:

- (a) commits a material breach of this Agreement that is incapable of remedy, or that is capable of remedy but is not remedied within thirty (30) days of written notice requiring it to be remedied (non-payment of an undisputed amount after the grace period in Section 12.11 is a material breach); or
- (b) enters administration, provisional liquidation or any composition or arrangement with its creditors; applies for or is subject to a moratorium under Part A1 of the Insolvency Act 1986; has a resolution passed or an order made for its winding up (other than for a solvent restructuring); has a receiver,

administrative receiver or manager appointed over any of its assets; or ceases, or threatens to cease, to carry on all or substantially all of its business.

19.4 Termination by Subcontext for Convenience

Subcontext may terminate this Agreement, or a Subscription, for convenience by giving Customer at least 90 days' written notice, or, for a Regulated Customer, the notice set out in Schedule 1, with a refund under Section 12.5. Where a Subscription has a Fixed Term, notice under this Section may not take effect before the end of that Fixed Term unless the Order Form allows it.

19.5 Effect of Termination

On the Termination Date: (a) Customer's right to use the Service (or the affected Organisation) ends; (b) all undisputed Fees accrued up to the Termination Date become payable; (c) unused Bought Credit is refundable as set out in Section 12.16, and any other refund due is paid under Section 12.5; (d) phone numbers assigned to the Organisation are released to the carrier under Section 7.5 unless Customer has asked to port them out, and connected domains stop serving; and (e) Customer Data is handled under Section 19.6. Termination does not affect rights and liabilities that have accrued by the Termination Date.

19.6 Export, Return and Deletion of Customer Data

Customer may export Customer Data at any time during the term using the export tools in the Service. Within thirty (30) days after the Termination Date, Customer may export Customer Data, or ask Subcontext in writing to return it in a commonly used machine-readable format or to delete it, and Subcontext will give reasonable assistance. Subcontext will delete Customer Data within ninety (90) days after the Termination Date, and automated database backups containing it expire within seven (7) days after that deletion. The following are kept for longer, and only for as long as stated:

- billing and payment records, for seven (7) years, to meet Subcontext's legal obligations;
- the compliance decision trail, for the retention period Customer configured (six (6) years by default), where Customer instructs it or the law requires it;
- the audit log, for two (2) years from each entry; and
- anything subject to a legal hold, until the hold ends.

Subcontext continues to protect anything it keeps in accordance with this Agreement and the DPA. Trial workspaces are deleted as described in Section 12.15. For a Regulated Customer, the exit arrangements in Schedule 1 also apply.

19.7 Survival

The following survive termination: Sections 2, 6.7, 9.1 (for the periods in Section 19.6), 9.5, 12 (for amounts accrued, refunds and billing disputes), 15, 16, 19.5, 19.6, 19.7, 20, 22 and 23, Schedule 1 (for its exit provisions), and any other provision that by its nature is intended to survive. The DPA survives as it provides.

20. Confidentiality

20.1 Confidential Information

"Confidential Information" means all non-public information disclosed by or for one party ("Discloser") to the other ("Recipient") in connection with this Agreement that is marked as confidential or that a reasonable person would understand to be confidential, including Customer Data, the terms of any Order Form, and Subcontext's non-public security information.

20.2 Exclusions

Information is not Confidential Information to the extent it: (a) is or becomes public other than through the Recipient's breach; (b) was lawfully known to the Recipient without a duty of confidence before disclosure; (c) is independently developed by the Recipient without use of the Discloser's Confidential Information; or (d) is lawfully received from a third party without a duty of confidence. Personal data within Customer Data remains protected by the DPA whether or not an exclusion applies.

20.3 Obligations

The Recipient will: use the Discloser's Confidential Information only to perform its obligations and exercise its rights under this Agreement; not disclose it except as permitted by Section 20.4; and protect it with at least the care it uses for its own confidential information of a similar kind, and no less than reasonable care.

20.4 Permitted Disclosures

The Recipient may disclose Confidential Information: (a) to its and its group companies' employees, officers, contractors, sub-processors and professional advisers who need to know it and are bound by duties of confidence no less protective than this Section 20; (b) where required by law, a court order or the rules of a stock exchange, giving the Discloser reasonable prior notice where the law allows; (c) to a regulator with jurisdiction over the Recipient, including the FCA, the PRA and the ICO, without notice where the regulator requires that; or (d) with the Discloser's prior written consent. The Recipient is responsible for anyone to whom it discloses Confidential Information under paragraph (a).

20.5 Duration, Return and Destruction

These obligations continue during this Agreement and for five (5) years after it ends, and indefinitely for trade secrets and for personal data. On the Discloser's written request after termination, the Recipient will return or destroy the Discloser's Confidential Information, except that it may keep copies required by law or held in routine backups until they expire, which remain subject to this Section 20. Customer Data is returned and deleted under Section 19.6.

20.6 Injunctive Relief

Damages may not be an adequate remedy for a breach of this Section 20, and the Discloser may seek injunctive or other equitable relief in addition to any other remedy.

21. Changes to the Service and to these Terms

21.1 Changes Subcontext May Make

Subcontext may update these Terms, the AUP, the DPA and the other documents listed in Section 23.1. Changes to Fees and Plans are governed by Section 12.12, and changes to sub-processors by the DPA. Subcontext publishes each new version, with a summary of what has changed, in the Service.

21.2 Materially Adverse Changes

For a change that is materially adverse to Customer, Subcontext will give at least thirty (30) days' notice by email to the Organisation's owners and in the dashboard before the change takes effect, unless a shorter period is required by law, a regulator or a third-party provider (in which case Subcontext will give as much notice as is practicable). Customer may terminate the affected Subscriptions by written notice given before the change takes effect, and will receive a pro rata refund of prepaid Fees and all unused Bought Credit under Section 12.5. Other changes, such as clarifications, changes required by law, and changes describing new features, take effect when published.

21.3 Acceptance

A User may be asked to accept a new version when they next use the Service, and does so on Customer's behalf. If Customer does not terminate under Section 21.2, the new version applies to Customer from its effective date.

21.4 Order Forms

Where Customer has an Order Form, the terms of that Order Form change only by written amendment signed by both parties. Where an Order Form fixes a version of these Terms or a document listed in Section 23.1, that version continues to apply to Customer until the Order Form's then-current term ends, unless the change is required by law.

22. Disputes, Governing Law and Jurisdiction

22.1 Escalation

If a dispute arises under or in connection with this Agreement, either party may give the other written notice of it. Senior representatives of both parties will meet (in person or remotely) within 14 days of the notice to try in good faith to resolve it. If the dispute is not resolved within 30 days of the notice, either party may start court proceedings. Nothing in this Section prevents either party from seeking urgent injunctive relief at any time.

22.2 Governing Law

This Agreement, and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it, is governed by the law of England and Wales.

22.3 Jurisdiction

The courts of England and Wales have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement.

23. General

23.1 Entire Agreement and Order of Precedence

This Agreement consists of these Terms (including Schedule 1), the Acceptable Use Policy, the Data Processing Agreement, any Order Form, and any service-specific terms that apply to a service Customer uses (such as the Nurture with AI Advisor Terms). It is the entire agreement between the parties about its subject matter and supersedes all earlier agreements, representations and understandings about it. Each party acknowledges that it has not relied on any statement, representation or warranty not set out in this Agreement, but nothing in this Section limits liability for fraud. If there is a conflict between these documents, they take precedence in this order:

1. the DPA, in relation to the processing of personal data;
2. an Order Form;
3. service-specific terms, for the service they cover;
4. these Terms (with Schedule 1 prevailing over the rest of these Terms for a Regulated Customer); and
5. the AUP.

An Order Form sets the commercial details of Customer's Subscription, such as the Plan, Fees, allowances, Fixed Term, renewal, payment terms and platform fee rate, and these apply as stated wherever these Terms refer to an Order Form. Otherwise, an Order Form overrides a provision of these Terms, the AUP or service-specific terms only where it expressly identifies the provision it changes; general or inconsistent wording in an Order Form that does not do so has no effect on them.

The Privacy Policy, the Cookie Policy and the Consumer Notice are information notices and do not form part of this Agreement. Terms in any purchase order or other document issued by Customer do not apply, even if Subcontext accepts or acknowledges it.

23.2 Relationship of the Parties

The parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture or agency between them, and neither party may bind the other.

23.3 Publicity

Neither party will use the other's name or logo in marketing or publicity without the other's prior written consent, which may be given by email and withdrawn on reasonable notice.

23.4 Assignment and Subcontracting

Neither party may assign or transfer its rights or obligations under this Agreement without the other's prior written consent (not to be unreasonably withheld), except that either party may assign this Agreement to a company in its group, or to a successor to all or substantially all of its relevant business, on written notice to the other. Subcontext may use subcontractors to provide the Service, subject to the DPA for sub-processors, and is responsible for their performance as for its own.

23.5 Notices

Notices under this Agreement must be in writing. Notices to Subcontext must be sent to hello@subcontext.com or by post to its registered office. Notices to Customer may be sent to the email addresses of its Organisations' owners, or by post to Customer's registered office or the business address

it has given. An email notice is treated as received when sent, or, if sent outside 09:00 to 17:30 on a business day in England, at 09:00 on the next business day, unless the sender receives a delivery failure message. A posted notice is treated as received on the second business day after posting by first class or recorded delivery. This Section does not apply to the service of court proceedings.

23.6 Waiver

A failure or delay by either party in exercising a right or remedy is not a waiver of it, and a single or partial exercise of a right or remedy does not prevent its further exercise.

23.7 Severability

If any provision of this Agreement is found invalid or unenforceable, it applies with the minimum modification needed to make it valid and enforceable, and the rest of this Agreement is unaffected.

23.8 Export Control and Sanctions

Customer confirms that it is not located in, and will not use the Service from, any country or territory subject to comprehensive UK, EU or US sanctions, and will not give access to the Service to any person or entity on a UK, EU or US sanctions list. Customer will comply with all applicable export control and trade sanctions laws in connection with its use of the Service.

23.9 Third-Party Rights

A person who is not a party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms, except that Apple and its subsidiaries may enforce Section 3.5 as it relates to an App obtained from Apple's App Store. The parties may vary or end this Agreement without the consent of any third party.

24. Contact

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

Schedule 1: Regulated Customers

1. When this Schedule Applies

This Schedule applies to Customer ("Regulated Customer") from the time Customer declares under Section 5.2 that it is authorised or regulated by the FCA, the PRA or another financial services regulator, or an Order Form says that it applies. Where this Schedule conflicts with the rest of these Terms, this Schedule prevails. In this Schedule, "Regulator" means the FCA, the PRA, and any other authority with regulatory jurisdiction over the Regulated Customer, including any person appointed by them.

2. Purpose

The parties recognise that a Regulated Customer may use the Service as an outsourcing arrangement, or to support an important business service, under the rules that apply to it (including the FCA's SYSC 8 and operational resilience rules, and for PRA-regulated firms the PRA's expectations on outsourcing and third-party risk management). Subcontext will cooperate with the Regulated Customer so that it can meet those rules in relation to the Service.

3. Access, Audit and Information Rights

(a) Subcontext will give the Regulated Customer, its internal and external auditors, and each Regulator effective access to: data relating to the Service provided to the Regulated Customer; Subcontext's personnel involved in providing it; and Subcontext's relevant premises, books and records, to the extent Subcontext controls them. For infrastructure operated by Subcontext's hosting provider, access is provided through that provider's own assurance reports and arrangements.

(b) Requests from a Regulator have no frequency or notice limits, and Subcontext will comply with them directly where the Regulator asks it to.

(c) Audits by the Regulated Customer or its auditors follow the DPA, except that the frequency and notice limits in the DPA do not apply after a Personal Data Breach or an operational incident under paragraph 6, where the information Subcontext has provided is reasonably insufficient to show compliance, or where a Regulator requires the audit.

(d) Each party bears its own costs of audits and information requests under this paragraph. Audits must be conducted so as to minimise disruption to Subcontext's business and must respect the confidentiality of other customers' data.

4. Sub-Processors and Subcontracting

Subcontext will give the Regulated Customer notice of material changes to its sub-processors, and the Regulated Customer may object, as set out in the DPA. Subcontext will also tell the Regulated Customer of any development that may have a material impact on Subcontext's ability to provide the Service effectively and in compliance with the law.

5. Business Continuity

The Service is hosted in one AWS region (Ireland, eu-west-1). Its application servers run across two availability zones and replace unhealthy servers automatically, and its database is backed up automatically with point-in-time recovery for seven (7) days. Subcontext maintains business continuity and disaster recovery plans with a recovery time objective of four (4) hours and a recovery point objective of twenty-four (24) hours, and tests them at least once a year. Summaries are published at /trust/business-continuity-disaster-recovery and /trust/operational-resilience-statement, and Subcontext will give the Regulated Customer a summary of the results of its tests on request.

6. Operational Incidents

In addition to Section 10.2, Subcontext will notify the Regulated Customer promptly, and in any event within 24 hours, after becoming aware of an operational incident that materially affects the availability, integrity or security of the Service provided to it, and will provide the information the Regulated Customer reasonably needs to manage the incident and to meet its own incident reporting obligations to a Regulator.

7. Consumer Duty Cooperation

Subcontext will cooperate with the Regulated Customer's monitoring of outcomes for its customers under the Consumer Duty, including by providing, on reasonable request, information about Agent behaviour, incidents and the AI models used by the Service. Subcontext will give advance notice of changes to the AI models used by the Regulated Customer's Agents where practicable, and otherwise notice as soon as practicable after the change.

8. Exit Assistance

For 90 days after the Termination Date ("Exit Period"), Subcontext will give the Regulated Customer reasonable assistance to transfer the Service to itself or a replacement provider, including: returning Customer Data in commonly used machine-readable formats (such as JSON and CSV); answering reasonable questions about data structures; and, if the Regulated Customer asks before the Termination Date, continuing to provide the Service on the existing terms and Fees for all or part of the Exit Period. Where the Service continues during the Exit Period, the Termination Date for Section 19.6 is the date that continued Service ends. The current exit plan is published at /trust/exit-plan-data-return.

9. Termination on Regulatory Grounds

The Regulated Customer may terminate this Agreement, or the affected Subscription, by written notice where a Regulator directs or requires it to do so, or where continuing would put it in breach of its regulatory obligations and Subcontext cannot remedy the position within a reasonable period. No early termination charge applies, and Subcontext will refund prepaid Fees and unused Bought Credit under Section 12.5.

10. Termination by Subcontext for Convenience

Subcontext may terminate this Agreement with a Regulated Customer for convenience only by giving at least 6 months' written notice.

11. Changes to the Regulated Customer's Status

The Regulated Customer must update its declaration under Section 5.2 promptly if its regulatory status changes, and must tell Subcontext if a Regulator raises with it any concern about its use of the Service, to the extent the law allows.

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.