Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the agreement between Subcontext Ltd, a company registered in England and Wales (Company No. 17019645) whose registered office is at 124 City Road, London, EC1V 2NX ("Subcontext"), and the Customer, made under the Terms of Service. It governs Subcontext's processing of personal data on Customer's behalf when it provides the Service. It applies automatically whenever Customer uses the Service, including on a trial or free plan and where a firm uses Nurture with AI under the Nurture with AI Advisor Terms. The person who accepts the Terms of Service on Customer's behalf also accepts this DPA on Customer's behalf.

For personal data, this DPA takes precedence over the Terms of Service and any other document that forms part of the agreement, as set out in Section 16.

1. Definitions and Interpretation

1.1 Definitions

Terms not defined here have the meanings given in the Terms of Service.

- **"Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach" and "Processing"** have the meanings given in the Data Protection Laws, and "process" and "processed" are read accordingly.
- **"Data Protection Laws"** means, in each case as amended, replaced or re-enacted from time to time: (a) the UK GDPR (as defined in section 3(10) of the Data Protection Act 2018) and the Data Protection Act 2018; (b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"); and (c) Regulation (EU) 2016/679 (the "EU GDPR") and the laws of EU member states that supplement it, to the extent they apply to Customer's processing of Protected Data through the Service (for example where Customer is established in the EU, or offers goods or services to, or monitors, individuals in the EU).
- **"Protected Data"** means Personal Data that Subcontext processes on Customer's behalf in providing the Service: Personal Data that Customer, its users or its Contacts submit to the Service, that the Service collects or generates for Customer, or that Subcontext receives from a third party (such as a Partner or a service Customer connects) for Customer. It does not include data Subcontext processes as a Controller under Section 2.3.
- **"Regulator"** means the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA), and any other body with regulatory authority over Customer's regulated activities.
- **"Restricted Transfer"** means a transfer of Protected Data that is restricted under Chapter V of the UK GDPR or, where it applies, Chapter V of the EU GDPR.
- **"Security Measures"** means the technical and organisational measures described in Annex E.
- **"Sub-Processor"** means a third party Subcontext engages to process Protected Data on Customer's behalf.
- **"Supervisory Authority"** means the Information Commissioner's Office ("ICO") and, where the EU GDPR applies, the competent supervisory authority under it.

- **"Termination Date"** has the meaning given in the Terms of Service.
- **"Usage Data"** means operational metrics about the Service only, such as message and call volumes, response times, costs and error rates.

1.2 Interpretation

In this DPA: "including" and similar words mean "including without limitation"; "writing" includes email; a reference to a law includes that law as amended or replaced; and where the EU GDPR applies, a reference to an article of the UK GDPR includes the corresponding article of the EU GDPR. The headings that name an article of the UK GDPR show where this DPA meets that article and do not limit the clause.

2. Scope and Roles

2.1 Customer as Controller

Customer is the Controller of Protected Data and decides the purposes and means of its processing through its configuration and use of the Service. Where Customer itself processes some Protected Data as a Processor for another Controller (for example a broker acting for an insurer), Customer confirms that its instructions to Subcontext, including the appointment of Subcontext and its Sub-Processors, are authorised by that Controller, and Subcontext acts as Customer's sub-processor for that data.

2.2 Subcontext as Processor

Subcontext is the Processor of Protected Data. The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of Data Subjects are described in Annexes A to D.

2.3 Subcontext as Controller

Subcontext is an independent Controller of personal data it processes for its own purposes. These are: managing Customer's account and its users' accounts, including sign-in, two-factor authentication and the record of who accepted which legal document; billing, payments and credit; Usage Data; securing the Service and preventing fraud and abuse; providing support; Subcontext's own website, marketing and its own website assistant; and meeting Subcontext's legal obligations. This DPA does not apply to that data, which is described in the Privacy Policy. Subcontext does not use Protected Data for its own purposes, except to derive Usage Data, which it uses only to operate, bill for, support and secure the Service.

2.4 AI Processing and No Training

The Service uses AI models to process Protected Data on Customer's instructions, including to run Customer's Agents, screen messages, extract facts, summarise records, detect signs of vulnerability, and power the dashboard assistant. In doing so:

- Subcontext does not use Protected Data or other Customer Content, whether or not anonymised or aggregated, to train or fine-tune any AI model, and does not allow its Sub-Processors to do so
- Text AI runs on AWS Bedrock, which does not store prompts or responses or use them to train models
- For voice calls, OpenAI does not train on API data but may retain it for up to 30 days for abuse monitoring, after which it is deleted
- The dashboard assistant is Subcontext's AI in the dashboard. It processes Protected Data only to carry out tasks a user of Customer's Organisation asks for, and it proposes write actions that take effect only

when a user approves them. That processing is processing on Customer's instructions under this DPA

3. Customer's Obligations

Customer will comply with the Data Protection Laws in its use of the Service. In particular, Customer is responsible for:

- Ensuring its instructions to Subcontext, and its configuration of the Service, comply with the Data Protection Laws
- Having a lawful basis for each processing purpose and, for special category and criminal offence data, the conditions described in Annex D
- Obtaining any consent PECR requires for marketing by email, SMS, WhatsApp or automated calls, and screening against the Telephone Preference Service and Corporate Telephone Preference Service where required (the Service's checks are a safeguard, not a substitute)
- Giving Data Subjects the privacy information the Data Protection Laws require. Customer may do this in part by linking to the Consumer Notice, which describes the Service's processing
- Complying with the ICO's Children's Code (the Age Appropriate Design Code) where it applies, and having a lawful basis for any data about children (for example children named as insured lives)
- Ensuring the Protected Data it provides was lawfully obtained and is accurate
- Responding to Data Subjects' requests, with Subcontext's help under Section 7
- Managing its own users, their roles and their two-factor authentication settings, and keeping its credentials, API keys and connected accounts secure
- Assessing, before and during its use of the Service, whether the Security Measures are appropriate for its processing. Customer confirms that, having regard to the nature of its Protected Data, it considers them appropriate at the date it accepts this DPA, and will tell Subcontext if that changes so the parties can discuss in good faith whether adjustments are needed

Nothing in this DPA relieves Customer of its own responsibilities under the Data Protection Laws.

4. Subcontext's Processing Obligations

4.1 Documented Instructions (Article 28(3)(a))

Subcontext will process Protected Data only on Customer's documented instructions, including with regard to Restricted Transfers, unless the law of the United Kingdom (or, where the EU GDPR applies, of the EU or an EU member state) requires otherwise. In that case Subcontext will tell Customer of that legal requirement before processing, unless that law prohibits it on important grounds of public interest.

Customer's documented instructions are: this DPA; the Terms of Service; Customer's configuration and use of the Service, including the settings, Agents, workflows, integrations and approvals its users set up, and the actions its users take or approve; and any further written instructions the parties agree. An instruction that would change the Service, or require work outside its normal functionality, needs the parties' written agreement, including on any fees.

4.2 Unlawful Instructions (Article 28(3), final paragraph)

Subcontext will tell Customer immediately if, in its opinion, an instruction infringes the Data Protection Laws. Subcontext may suspend the processing concerned until the instruction is confirmed in writing,

changed, or withdrawn.

4.3 Confidentiality (Article 28(3)(b))

Subcontext will ensure that every person it authorises to process Protected Data, including its staff and contractors, is bound by a written duty of confidentiality or an appropriate statutory duty, and accesses Protected Data only as needed to provide, support and secure the Service, to give support Customer has asked for, to investigate a security or operational issue, or as the law requires.

4.4 Processor Duties

Subcontext will keep a record of its processing activities for Customer as Article 30(2) of the UK GDPR requires, cooperate with the Supervisory Authority on request, and comply with the obligations the Data Protection Laws place directly on processors. Subcontext will notify Customer promptly if it can no longer meet its obligations under this DPA. Customer may then give amended instructions, suspend the affected processing or, if the matter cannot be resolved, terminate the affected Service under the Terms of Service.

5. Security (Article 28(3)(c) and Article 32)

5.1 Security Measures

Subcontext will implement and maintain appropriate technical and organisational measures to protect Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, and the risks to Data Subjects. These include the Security Measures in Annex E. Subcontext's security policies are published at /trust.

5.2 Changes to the Security Measures

Subcontext may update the Security Measures as technology and threats change, provided that an update does not materially reduce the overall level of protection of Protected Data.

6. Sub-Processors (Article 28(2) and 28(3)(d))

6.1 Authorisation

Customer gives Subcontext general written authorisation to engage Sub-Processors. The Sub-Processors currently engaged by Subcontext are:

Sub-Processor	Location	Purpose
Amazon Web Services (AWS)	EU (Ireland), US	Cloud hosting, storage, compute, email delivery (SES)
AWS Bedrock (Anthropic models)	EU (Ireland, with AWS EU cross-region routing)	AI model inference for Agent responses and content analysis
AWS Bedrock (DeepSeek models)	UK (London)	AI model inference
Twilio	United States	SMS, WhatsApp and voice delivery, phone numbers, and verification codes

Sub-Processor	Location	Purpose
Stripe	United States	Payment processing
OpenAI	United States	Real-time speech, transcription and speech synthesis for voice calls
ElevenLabs	United States	Speech synthesis for voice calls
Meta Platforms	Ireland / United States	WhatsApp Business messaging, and Ads conversion reporting only where connected by Customer
Persona (via Twilio)	United States	Identity checks for phone number compliance registration
Data8	United Kingdom	Address lookup, phone number validation and Telephone Preference Service checks
Iress	United Kingdom	Whole-of-market insurance quoting, only where enabled by Customer
Google	United States	Calendar and Sheets, and Google Ads conversion reporting, only where connected by Customer
Apple	United States	Push notifications to the Subcontext iOS and Mac apps
Google Firebase	United States	Push notifications and crash reporting for the Subcontext Android app

This table is the definitive list. Subcontext also publishes it, with the data categories each Sub-Processor receives, at /trust/sub-processor-list; if the two differ, this table prevails. Sub-Processors marked "where enabled" or "where connected" receive Protected Data only if Customer turns on the related feature or connects the related account, and voice providers receive it only if Customer uses voice.

Services that Customer chooses and connects under its own agreements with their providers, such as its own policy administration or CRM systems connected through a custom integration, are not Sub-Processors. Subcontext sends data to them on Customer's instruction, and Customer's agreements with those providers govern what they do with it.

6.2 New Sub-Processors

Subcontext will give Customer at least thirty (30) days' notice before engaging a new Sub-Processor, or changing the location or purpose of an existing one in a way that materially affects Protected Data (the "Notice Period"). Notice will be given by email to the owners of Customer's Organisation and in the dashboard, and will say who the Sub-Processor is, where it processes data, and what it does.

6.3 Right to Object

Customer may object to a new or changed Sub-Processor on reasonable data protection grounds by writing to hello@subcontext.com within the Notice Period. The parties will discuss the objection in good faith. Subcontext may offer a solution, such as not enabling the feature that relies on that Sub-Processor for Customer, using an alternative, or adding safeguards. Until the objection is resolved, Subcontext will not use the new Sub-Processor for Customer's Protected Data where it is reasonably able to avoid doing so. If no solution acceptable to Customer is found within thirty (30) days of the objection, Customer may terminate the affected Service by written notice, without penalty, and Subcontext will refund prepaid Fees

for the period after termination and any unused Bought Credit. If Customer does not object within the Notice Period, the change is treated as authorised.

6.4 Sub-Processor Terms (Article 28(4))

Before a Sub-Processor processes Protected Data, Subcontext will carry out appropriate due diligence on it and put in place a written contract that imposes data protection obligations which, in substance, are no less protective than those in this DPA, so far as they apply to the services the Sub-Processor provides, and in particular sufficient guarantees of appropriate technical and organisational measures. Subcontext remains fully liable to Customer for the performance of each Sub-Processor's obligations, subject to Section 14.

Some providers also process some data as independent Controllers for their own legal and service purposes under their own terms (for example Stripe for fraud prevention and its regulatory obligations, and Meta for operating WhatsApp). Where Customer connects its own advertising account for conversion reporting, Customer's own agreement with Google or Meta governs how they use that data.

7. Data Subject Rights (Article 28(3)(e))

7.1 Assistance

Taking into account the nature of the processing, Subcontext will assist Customer by appropriate technical and organisational measures, so far as possible, to respond to requests from Data Subjects exercising their rights under Chapter III of the UK GDPR, including the rights of access, rectification, erasure, restriction, portability and objection, and the right not to be subject to solely automated decisions. The Service provides self-service tools for this, including exports, record editing, a lead erasure tool and data-rights request tracking. Where Customer cannot fulfil a request with those tools, Subcontext will help on request.

This assistance is free of charge, except that Subcontext may charge reasonable costs, agreed with Customer in advance, for assistance that is manifestly excessive or repetitive.

7.2 Requests Received by Subcontext

If Subcontext receives a request from a Data Subject about Protected Data, it will forward the request to Customer promptly and in any event within 5 business days, and will not respond to the Data Subject itself, except to direct them to Customer, unless Customer instructs it to or the law requires it.

7.3 Consent, Objections and Suppression

Customer instructs Subcontext to:

- Record each decision a Data Subject makes about being contacted, and each decision Customer records for them, with the purpose, channel, lawful basis, the wording in force, where it was given and supporting evidence (such as the time, IP address and browser), and to check every message against those records and Customer's consent settings before sending it
- Operate, on Customer's behalf, a preference page linked from Customer's messages and one-click unsubscribe from email, and act on the choices Data Subjects make there, on STOP replies, on unsubscribe replies and on spam complaints, without further instruction

- When Customer erases a Data Subject's record, remove the identifying evidence from their consent records and, for each purpose and channel they refused or withdrew, keep a keyed one-way digest of the email address or phone number concerned (never the address or number itself), held separately for Customer's Organisation, so that their objection is applied again if the same address or number is added later. These digests are kept for as long as Customer's Organisation uses the Service and are deleted with the rest of the Protected Data under Section 13. Customer is responsible for determining that this retention is necessary to respect the Data Subject's objection.

8. Assistance with Security, Breaches and Impact Assessments (Article 28(3)(f))

Taking into account the nature of the processing and the information available to it, Subcontext will assist Customer to meet its obligations under Articles 32 to 36 of the UK GDPR: security of processing; notifying Personal Data Breaches to the Supervisory Authority and to Data Subjects; data protection impact assessments; and prior consultation with the Supervisory Authority. Subcontext publishes its own Data Protection Impact Assessment and Transfer Risk Assessment to support Customer's own assessments, and will answer Customer's reasonable questions about the processing.

This assistance is free of charge, except that Subcontext may charge reasonable costs, agreed with Customer in advance, for assistance that is manifestly excessive or repetitive.

9. Personal Data Breaches (Article 33)

9.1 Notification

Subcontext will notify Customer of a Personal Data Breach affecting Protected Data without undue delay, and in any event within 48 hours, after becoming aware of it. Notice will go by email to the owners of Customer's Organisation and to any security contact Customer has given Subcontext. Subcontext becomes aware of a breach when it has a reasonable degree of certainty that a security incident has led to Protected Data being compromised.

9.2 Content

The notice will include, so far as the information is available:

- A description of the nature of the breach, including the categories and approximate number of Data Subjects and records concerned
- The name and contact details of the person at Subcontext from whom more information can be obtained
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach and reduce its possible adverse effects

Where it is not possible to provide all the information at once, Subcontext will provide it in phases without undue further delay, and will keep Customer updated until the breach is resolved.

9.3 Response and Cooperation

Subcontext will promptly take reasonable steps to contain, investigate and remedy the breach and reduce its effects, and will cooperate with Customer, and with any Supervisory Authority or Regulator, in its

investigation. Customer decides whether to notify the Supervisory Authority, a Regulator or Data Subjects. Subcontext will not notify them about a breach of Protected Data, or make any public statement naming Customer, without Customer's prior agreement, unless the law requires it. Subcontext will keep a record of every Personal Data Breach affecting Protected Data, including its facts, effects and the remedial action taken, and make it available to Customer on request. Notifying or responding to a breach is not an admission of fault or liability.

Operational incidents that materially affect the Service but are not Personal Data Breaches are covered by the Regulated Customers schedule in the Terms of Service, where it applies.

10. International Transfers

10.1 Where Protected Data Is Processed

Protected Data is hosted by AWS in Ireland (eu-west-1). Text AI runs on AWS Bedrock in the EU (Ireland, eu-west-1, whose EU cross-region routing may serve a request from another AWS EU region) or London (eu-west-2), and requests to AI models routed to the United States are refused. Voice AI (OpenAI and ElevenLabs), messaging (Twilio and Meta), payments (Stripe) and app push notifications (Apple and Google Firebase) involve providers in the United States, as do the other United States Sub-Processors in Section 6.1 where Customer uses the related feature. Customer authorises these transfers as part of its documented instructions.

10.2 Safeguards

Transfers to the European Economic Area rely on the UK's adequacy regulations. Subcontext will make Restricted Transfers to the United States only where:

- The recipient is certified under the UK Extension to the EU-US Data Privacy Framework (the UK-US data bridge); or
- Otherwise, under the UK International Data Transfer Agreement, or the EU Standard Contractual Clauses with the UK Addendum, issued by the ICO, together with any supplementary measures the Transfer Risk Assessment identifies

Subcontext's Transfer Risk Assessment records the transfers, the mechanism used and the supplementary measures.

Where the EU GDPR applies to Customer's processing, transfers of Protected Data from the EU to Subcontext in the United Kingdom rely on the European Commission's adequacy decision for the United Kingdom while it is in force. If it ceases to apply, the parties will enter into the EU Standard Contractual Clauses (module 2, or module 3 where Customer is a processor) for those transfers, which will be treated as incorporated into this DPA.

10.3 Changes

Subcontext will tell Customer without undue delay if a transfer mechanism it relies on ceases to be valid (for example if a Sub-Processor loses its Data Privacy Framework certification) and will put an alternative mechanism in place or stop the transfer. If neither is possible, Customer may suspend the affected feature or terminate the affected Service on the terms in Section 6.3. Subcontext will not make a new kind of Restricted Transfer except under Section 6.2.

11. Audits and Information (Article 28(3)(h))

11.1 Information

Subcontext will make available to Customer all information necessary to demonstrate compliance with this DPA and Article 28 of the UK GDPR. On request, and without charge, Subcontext will provide:

- A technical and security summary of the Service
- Completed responses to Customer's reasonable security and due diligence questionnaires
- Its security and data protection policies, published at /trust, including the Sub-Processor List, the Data Protection Impact Assessment and the Transfer Risk Assessment
- Records of restore tests and incident response exercises, in summary
- Reports of external penetration tests, once those tests have begun (they are planned from 2027), with reasonable redaction

Subcontext does not currently hold an independent certification such as ISO 27001 or a SOC 2 report, and will tell Customer if that changes.

11.2 Audits and Inspections

Customer, or an independent auditor it appoints who is not a competitor of Subcontext, may audit and inspect Subcontext's compliance with this DPA. Ordinarily, an audit is limited to once in any twelve (12) months, on at least thirty (30) days' written notice, during business hours and without unreasonable disruption to the Service, and the auditor signs a reasonable confidentiality undertaking first. Those limits on frequency and notice do not apply where:

- A Personal Data Breach affecting Customer's Protected Data has occurred;
- The information provided under Section 11.1 is reasonably insufficient to demonstrate compliance;
- A Supervisory Authority or Regulator requires or asks for the audit; or
- The Data Protection Laws or Customer's regulatory obligations require it

in which case Subcontext will cooperate on such notice as is reasonable in the circumstances. Subcontext may protect the confidentiality of its other customers' data and its security (for example by not giving direct access to shared systems), and will provide equivalent evidence wherever it does so. Each party bears its own costs of an audit, except that Subcontext may charge its reasonable costs, agreed in advance, for audits beyond one in twelve months that are not within the exceptions above. Subcontext will remedy any non-compliance an audit identifies without undue delay.

11.3 Supervisory Authorities and Regulators

Subcontext will cooperate with the ICO, the FCA, the PRA and any other Supervisory Authority or Regulator with authority over Customer. Each of them has the same rights of access, information, audit and inspection as Customer under this Section 11, exercisable directly, at any time, and without the frequency, notice or confidentiality-undertaking conditions in Section 11.2 except as the authority itself agrees. Where Customer has declared it is regulated, the Regulated Customers schedule in the Terms of Service gives further rights.

12. Government and Other Third-Party Requests

If Subcontext receives a legally binding request from a public authority, court or other third party for access to Protected Data (other than a request from Customer's Supervisory Authority or Regulator under Section 11.3), Subcontext will:

- Try to redirect the requester to Customer
- Notify Customer promptly, giving a copy of the request where possible, so that Customer can seek a protective order or other remedy, unless the law prohibits notice. Where notice is prohibited, Subcontext will use reasonable efforts to obtain a waiver of the prohibition
- Review the lawfulness of the request and challenge it where, after careful assessment, there are reasonable grounds to consider it unlawful
- Disclose only the minimum Protected Data needed to comply with the request, and keep a record of what was requested and disclosed

Subcontext will not give any public authority voluntary or general access to Protected Data, and has not built any means for doing so into the Service.

13. Deletion and Return of Protected Data (Article 28(3)(g))

13.1 During the Agreement

Customer can export its Protected Data at any time through the dashboard, the REST API and the MCP server, and can delete it. Some Protected Data is deleted automatically during the agreement under the retention periods in Annex A, Part 3.

13.2 At the End of the Agreement

The deletion clock is set out in the Terms of Service and runs from the Termination Date. In summary, Customer may export its Protected Data, or elect in writing to have it returned or deleted, within thirty (30) days of the Termination Date. On request within that period, Subcontext will return the Protected Data in a structured, commonly used, machine-readable format (such as JSON and CSV), as described in the Exit Plan & Data Return Policy. Subcontext will then delete all Protected Data, and existing copies, within ninety (90) days of the Termination Date, and automated database backups containing it expire within seven (7) days after that deletion. Data held by Sub-Processors is deleted under their contractual obligations. Subcontext will confirm deletion in writing on request. Return and deletion under this Section 13 are free of charge, and the return of Protected Data is not conditional on the settlement of any dispute about Fees.

13.3 Data Kept Longer

Subcontext keeps the following beyond the deletion date, but only where listed and for the stated reason:

Data	Kept for	Reason
Billing and payment records, including payment provider event records	7 years	Legal obligation (tax and accounting records)
The compliance decision trail	The retention period Customer has configured (6 years by default)	Where Customer instructs it, or the law requires it

Data	Kept for	Reason
The audit log	2 years from each entry	Security, accountability and evidence of how Protected Data was handled
Any data under a legal hold	Until the hold is lifted	A legal claim, regulatory investigation, complaint or incident investigation

While it keeps any Protected Data, Subcontext will continue to protect it under this DPA and process it only for the purpose for which it is kept. Data in backups is never restored into live use without deletions being applied again.

14. Liability

Each party's liability arising out of or in connection with this DPA, and Subcontext's liability for breach of the Data Protection Laws, is subject to the limitations and exclusions of liability in the Terms of Service. Subcontext's liability for breach of this DPA or the Data Protection Laws falls under the separate data protection liability cap set out there, and not the general cap. Nothing in this DPA limits either party's liability where the law does not allow it to be limited, or limits a Data Subject's rights against either party under the Data Protection Laws. Where both parties are responsible for damage caused by processing, each is liable to the other only for the part of the damage that corresponds to its share of responsibility, consistent with Article 82 of the UK GDPR.

15. Duration, Survival and Changes

15.1 Duration and Survival

This DPA applies for as long as Subcontext processes Protected Data, including after the Termination Date until all Protected Data has been returned or deleted under Section 13. Sections 9, 11, 12, 13 and 14 survive for that period and, for Section 14, afterwards.

15.2 Changes

Subcontext may change this DPA under the changes clause of the Terms of Service, which requires advance notice of changes that are materially adverse to Customer and gives Customer a right to terminate before they take effect. Subcontext may also make changes the Data Protection Laws or a Supervisory Authority require, including to adopt new standard clauses or transfer mechanisms, with as much notice as is practicable. Where Customer has a signed order form or Enterprise agreement, this DPA changes only as that agreement allows.

16. Precedence, Governing Law and Jurisdiction

For personal data, this DPA prevails over any conflicting term of the Terms of Service, an order form or any other document forming part of the agreement, except that the UK International Data Transfer Agreement, the UK Addendum or the EU Standard Contractual Clauses prevail over this DPA where they apply. This DPA is governed by the laws of England and Wales, and the courts of England and Wales have exclusive jurisdiction over any dispute arising out of or in connection with it, except where the EU Standard Contractual Clauses require another law or forum for disputes under them.

Annex A: Description of Processing

Part 1: Subject Matter, Duration, Nature and Purpose

- **Subject matter:** the provision of the Subcontext platform to Customer: AI agents that converse with Customer's Contacts on web chat, SMS, WhatsApp, email and voice; a CRM with outreach and workflows; insurance quoting, applications, policies and claims; payments; integrations; the REST API and MCP server; the mobile and desktop apps; and the dashboard assistant
- **Duration:** the term of the agreement, then until the Protected Data is returned or deleted under Section 13
- **Frequency:** continuous
- **Nature:** collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, analysis by AI models, use, disclosure by transmission (to Sub-Processors, and to systems and recipients Customer directs), alignment and combination, restriction, erasure and destruction
- **Purpose:** to provide the Service to Customer as Customer configures and uses it, including support, security and the maintenance of the Service

Part 2: Processing by Service Area

Service area	What the processing involves
Conversations and Agents	Receiving, storing and sending messages with Contacts on web chat (including embedded widgets, quote forms, hosted mini-sites and Customer's custom domains), SMS, WhatsApp and email; generating Agent replies with AI; screening inbound messages with guardrails; handing conversations to Customer's team
Voice	Handling inbound and outbound calls, real-time speech recognition and synthesis, call recording (where Customer enables it), transcripts and call summaries
AI analysis	Extracting facts into the CRM, summarising leads and conversations, scoring leads, applying conduct rules (including FCA conduct, Consumer Duty, medical disclosure, vulnerable customers, complaints handling, financial promotions and data protection), recording compliance decisions, and detecting signs that a person may be vulnerable (which flags the person, holds back sales and outreach, and alerts Customer's team)
CRM and outreach	Storing leads, contacts, pipelines, activities, tasks and notes; importing and receiving leads from Customer's systems and Partners; running outreach campaigns, workflows, scheduled follow-ups, callbacks, referrals and loyalty programmes; Nurture with AI campaigns for advisers' clients, including receiving an adviser's quote from a Partner such as Iress and adding the quoted products the adviser chooses to the client's email
Consent and suppression	Recording consent decisions and evidence, operating the preference page and unsubscribe, checking messages against consent, quiet hours and Telephone Preference Service results, and keeping suppression digests (Section 7.3)
Insurance	Collecting quote and application information, pricing quotes (including whole-of-market quoting through Iress where enabled), issuing and administering policies and their documents, and handling claims and complaints
Payments	Taking card payments through Stripe and setting up Bacs Direct Debit mandates, storing bank details encrypted, and recording payment status

Service area	What the processing involves
Lookups and validation	Address lookup, phone number validation and Telephone Preference Service checks through Data8
Connected services	Booking appointments in Google Calendar, writing rows to Google Sheets, ads conversion reporting with hashed contact details, and exchanging data with Customer's own systems through integrations and webhooks, in each case only where Customer connects them
Phone number compliance	Submitting Customer's business and representative details for regulatory registration of phone numbers, including identity checks through Persona via Twilio
Access and apps	Making Protected Data available to Customer's users in the dashboard, the iOS, Android and Mac apps (including push notifications), the REST API and the MCP server, and through the dashboard assistant
Analytics and exports	Producing reports, analytics, page-view statistics on Customer's sites, and exports for Customer
Support and security	Investigating issues Customer raises, monitoring errors and performance, and keeping logs needed to secure the Service and show who did what

Part 3: Retention During the Agreement

Unless Customer deletes it sooner, Protected Data is kept for the agreement and deleted under Section 13, except for the following, which the Service deletes or scrubs automatically:

Data	Kept for
Visitor IP addresses and browser details on conversations and enquiries	90 days (1 year where the conversation was escalated or flagged as spam)
Page-view analytics, voice call events and inbound email logs	1 year
Voice call recordings	365 days by default, or as Customer configures; recordings under legal hold are kept until it is lifted
Raw lead data received from Customer's systems	365 days by default, or as Customer configures
Lead activity events	180 days by default, or as Customer configures
Compliance decision trail	6 years by default, or as Customer configures between 3 and 25 years
Audit log and email delivery logs	2 years
AI model call logs	13 months
API request logs	3 months
Integration request logs and application error reports	90 days
Inbound email held for processing	30 days
Quotes handed over by a Partner for Nurture with AI that do not lead to a message	30 days

Data	Kept for
Performance monitoring data	10 days
Data exports	7 days

Conversations close automatically after 7 days without activity; closing does not delete them.

Annex B: Categories of Data Subjects

- **Prospects and enquirers:** people who contact Customer, visit Customer's sites or widgets and interact with them, or are introduced to Customer as leads
- **Applicants and proposers** for insurance, and other people named in a quote or application, such as joint applicants, named drivers, dependants and lives assured (who may include children)
- **Policyholders and insured persons,** and beneficiaries
- **Claimants,** and third parties named in a claim
- **Payers,** including Direct Debit account holders who are not the policyholder
- **Callers and call recipients** on Customer's voice channels
- **Outreach recipients:** people Customer contacts by SMS, WhatsApp, email or phone, including people referred by a friend
- **Clients of advisers** using Nurture with AI, including identifiers and quotes received from a Partner such as Iress, and the other people named in such a quote
- **Complainants** whose complaints Customer records in the Service
- **Customer's personnel and representatives,** to the extent they appear in Protected Data (for example as the owner of a conversation or task, or as a business representative in a phone number compliance registration)
- **Any other individual** whose personal data appears in content that Customer or a Contact submits

Annex C: Categories of Personal Data

- **Identity:** names, titles, dates of birth, age, sex recorded at birth, external and Partner identifiers, and the FCA individual reference numbers of Customer's advisers
- **Contact details:** email addresses, phone numbers, postal addresses and postcodes
- **Personal circumstances:** occupation, employment and income, marital status, smoker status, height and weight, residence, property, vehicle, travel and other details needed to quote for the product concerned
- **Insurance records:** quotes (including quotes a Partner hands over, with their insurers, products, prices and cover amounts), applications and their answers, underwriting outcomes, policies, policy documents, renewals, claims and their evidence
- **Financial data:** payment amounts, dates and status, and Bacs Direct Debit bank account details (sort code, account number and account holder name, stored encrypted). Card details are handled by Stripe and never stored by Subcontext
- **Communications content:** messages, emails and attachments on every channel, call audio, call recordings, transcripts and summaries

- **AI-generated data:** Agent replies, extracted facts, summaries, lead scores, guardrail and conduct-rule outcomes, compliance decisions, and vulnerability flags
- **CRM data:** lead status and pipeline stage, activities, tasks, notes, campaign and outreach membership, follow-ups, callbacks, referrals, loyalty membership, and reasonable adjustments recorded for a person
- **Consent records:** each decision about being contacted, with its purpose, channel, lawful basis, the wording shown, where and when it was given and supporting evidence (such as IP address and browser)
- **Suppression digests:** keyed one-way digests of the email addresses or phone numbers of erased Data Subjects who refused or withdrew (Section 7.3)
- **Lookup results:** address matches, phone number validation results and Telephone Preference Service status
- **Connected service data:** calendar bookings, spreadsheet rows, hashed contact details sent for ads conversion reporting, and data exchanged with Customer's systems
- **Identity verification data:** details of Customer's business representatives submitted for phone number compliance registration
- **Complaints and data rights records:** complaint details, deadlines and outcomes, and requests from Data Subjects and how they were handled
- **Technical data:** IP addresses, browser and device information, visitor and session identifiers, pages viewed on Customer's sites, and log entries

Annex D: Special Category and Criminal Offence Data

D.1 What Is Processed

Insurance quoting and applications routinely involve special category data, and the Service is designed to process it. In particular:

- **Health data:** medical history, conditions, medication, disabilities, smoker status, height and weight, and other health questions asked for life, critical illness, income protection, health, travel and similar products, health information in claims, and the underwriting details in a quote a Partner hands over for Nurture with AI
- **Health inferred from circumstances:** vulnerability flags and reasonable adjustments may reveal health or disability
- **Other special category data:** may appear in conversations or claims where a Contact chooses to share it
- **Criminal offence data:** unspent convictions, including motoring convictions, where an insurance application asks for them

Voice recordings are kept as a record of the call. The Service does not use them, or any other data, to identify a person by their voice or other biometric characteristics.

D.2 Safeguards Subcontext Applies

- Text AI processing of this data takes place in the UK and EU on AWS Bedrock. It may reach United States providers where a Contact gives it by SMS, WhatsApp or a voice call (Section 10)

- An Agent tool records a Contact's explicit consent to the processing of health data, and conduct rules govern how Agents ask about medical information and treat people who may be vulnerable
- Bank details and other sensitive fields are encrypted in the application, in addition to database encryption, and access follows Customer's user roles (Annex E)
- A quote a Partner hands over for Nurture with AI is encrypted in the application, its health details are shown only to the adviser who received it and never included in a message to the client, and it is deleted after 30 days unless it leads to a message (Annex A, Part 3)
- This data is never used to train AI models (Section 2.4)

D.3 Customer's Responsibilities

Customer instructs Subcontext to process special category and criminal offence data only as necessary to provide the Service. Customer is responsible for identifying that it processes this data; having an Article 9 condition and, where relevant, a condition in Schedule 1 to the Data Protection Act 2018 (such as the insurance condition), and an appropriate policy document; obtaining explicit consent where that is the condition it relies on; carrying out any data protection impact assessment needed; and limiting the questions its Agents and forms ask to what is necessary.

Annex E: Technical and Organisational Security Measures

These measures describe the Service on the date of this DPA. Further detail is in the policies published at /trust.

E.1 Governance and People

- A designated Security Officer, a member of the founding team, owns the security programme and reports to the directors
- Security policies are approved by the directors and reviewed at least annually
- Staff and contractors sign confidentiality agreements before receiving access, have background checks proportionate to their role, and complete security awareness training at onboarding and at least annually
- Suppliers and Sub-Processors are assessed before engagement and reviewed periodically

E.2 Hosting and Network

- Hosted on AWS in Ireland (eu-west-1). Application and background servers run in private network subnets across two availability zones, scale automatically, are replaced automatically if they fail health checks, and run containers as a non-root user
- An AWS web application firewall applies managed rule sets (common exploits, SQL injection, known bad inputs, IP reputation, Linux and Unix attacks) and a per-IP rate limit; application rate limits apply to sign-in and other features
- Network flow logs, firewall logs and application logs are kept for 30 days
- Infrastructure is defined as code and version-controlled

E.3 Encryption

- In transit: TLS 1.2 or higher (TLS 1.3 supported) for all web traffic, with HTTP redirected to HTTPS and HTTP Strict Transport Security; TLS required for connections to the database and cache, and used for

connections to Sub-Processors

- At rest: the whole database and its backups (AES-256, managed by AWS), the cache, file storage (AES-256) and container images are encrypted
- Application-level encryption (AES-256-GCM) is added for integration credentials and secrets, webhook secrets, settings, contact verification details, phone account tokens, Direct Debit bank details, and quotes and signing secrets for Partner handoffs
- Production secrets are held in AWS Secrets Manager and encrypted credentials, never in source code. Passwords are hashed with bcrypt, and API tokens and client secrets are stored hashed

E.4 Access Control

- Each Customer's data is separated by Organisation; users see only the Organisations they belong to
- Customer users hold one of three roles (owner, manager, user); sensitive actions such as erasing a lead are limited to owners and managers and require a reason
- Two-factor authentication (authenticator codes, backup codes or in-app sign-in approval) is enforced by default for new Organisations and always for Subcontext's administrators
- Accounts lock for 10 minutes after 3 failed sign-in attempts; password reset links expire after 6 hours; sessions expire after 30 days of inactivity, and changing a password or turning off two-factor authentication ends other sessions
- API and app access uses OAuth 2.0 with PKCE, scoped access and access tokens that expire after 2 hours
- Subcontext staff access Protected Data only for the reasons in Section 4.3. When an administrator acts within Customer's account, the start, the end and every action are recorded against that administrator
- Privileged access is reviewed at least quarterly and removed within 24 hours of a person leaving

E.5 Logging, Monitoring and Integrity

- An audit log records significant actions (who, what, when, IP address, browser and request, and any administrator acting on a user's behalf). Entries cannot be changed once written and are kept for 2 years
- Compliance decisions are recorded in a hash-chained trail sealed every minute, which refuses to be purged if the chain is broken
- Webhooks from Twilio, Stripe, AWS SES and integrations are signature-verified and rejected if verification fails
- Passwords, tokens and other sensitive values are filtered from logs, and sensitive values given to AI tools are stored redacted
- Application errors raise email alerts when they first occur, recur or increase; infrastructure alarms cover the database, cache, load balancer and application servers; a daily heartbeat confirms scheduled processing

E.6 Secure Development and Change

- Before release, the full check suite runs: code style and security static analysis (Brakeman, failing on any warning), dependency audits for Ruby and JavaScript, and the automated test suites with a 100% line and branch coverage requirement

- Production releases pass a manual approval stage in the deployment pipeline; database migrations run before rollout and stop the release if they fail; previous releases can be redeployed
- Container images are immutable and scanned for vulnerabilities when published; automated dependency updates are raised weekly
- The web application uses CSRF protection, a strict Content Security Policy and security headers
- Vulnerabilities are remediated against set targets (Critical 24 hours, High 7 days, Medium 30 days, Low 90 days). External penetration testing is planned at least annually from 2027, and researchers can report issues under the Vulnerability Disclosure Policy

E.7 Availability and Recovery

- The database has automated backups with point-in-time recovery for 7 days, and deletion protection
- Recovery time objective 4 hours and recovery point objective 24 hours for the core platform; restoration is tested at least annually
- Maintenance mode and an emergency lockdown at the load balancer protect data while recovery work is done
- The database runs in a single availability zone and the Service in a single AWS region; recovery relies on backups and point-in-time recovery rather than a standby database or second region

E.8 Incident Response

- An Incident Response Plan covers detection, containment, eradication, recovery, notification and post-incident review, and is tested at least annually
- Customers are notified of Personal Data Breaches under Section 9

E.9 AI Safeguards

- Baseline guardrails against prompt injection, jailbreak attempts and system prompt extraction run on every inbound message and cannot be turned off; content from outside the platform is treated as untrusted and kept separate from instructions
- A compliance policy gate checks Agent actions; conduct rules, vulnerability detection, human escalation and review, tool approvals and an optional AI disclosure rule are available for Customer to configure; Customers test Agents before they go live
- Text AI runs only in UK and EU regions; Protected Data is not used to train models (Section 2.4)

E.10 Data Minimisation, Retention and Data Subject Rights

- Only the data a Sub-Processor needs is sent to it; contact details for ads conversion reporting are hashed before they are sent
- Retention periods are enforced automatically (Annex A, Part 3)
- Self-service exports, record editing, a lead erasure tool (which refuses erasure while a policy is live, an application is in progress or a claim exists) and data-rights request tracking help Customer meet Data Subjects' requests
- Card details are never stored by Subcontext; payments are handled by Stripe

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.