Sub-Processor List

The following third-party sub-processors are engaged by Subcontext Ltd to process data on behalf of customers.

1. About This List

A sub-processor is a third party that Subcontext engages to process personal data on behalf of its customers, where Subcontext is the customer's processor. This list is published so customers can see who handles their data, where, and for what purpose, as required by the Data Processing Agreement and Article 28 of the UK GDPR.

Some sub-processors are used only when a customer enables the related feature or connects the related service. Where that is the case, it is stated in the Purpose column.

2. Current Sub-Processors

Sub-Processor	Location	Purpose	Data Categories
Amazon Web Services (AWS)	EU (Ireland), US	Cloud hosting, compute, storage, email delivery (SES)	All customer data
AWS Bedrock (Anthropic models)	EU (Ireland, with AWS EU cross-region routing)	AI model inference for Agent responses and content analysis	Conversation content, knowledge base content
Twilio	United States	SMS, WhatsApp and voice delivery, phone numbers, and verification codes	Contact phone numbers, message content, call audio
Stripe	United States	Payment processing	Customer billing data, transaction amounts
AWS Bedrock (DeepSeek models)	UK (London)	AI model inference	Conversation content, knowledge base content
OpenAI	United States	Real-time speech, transcription and speech synthesis for voice calls	Call audio, conversation content
ElevenLabs	United States	Speech synthesis for voice calls	Agent response text
Meta Platforms	Ireland, United States	WhatsApp Business messaging	Contact phone numbers, message content
Persona (via Twilio)	United States	Identity checks for phone number compliance registration	Customer business representative identity data
Data8	United Kingdom	Address lookup, phone number validation and Telephone Preference Service checks	Postcodes, addresses, phone numbers

Sub-Processor	Location	Purpose	Data Categories
Iress	United Kingdom	Whole-of-market insurance quoting, where enabled by the Customer	Applicant details needed to quote
Google	United States	Calendar and Sheets, and Google Ads conversion reporting, only where connected by the Customer	Booking details, sheet rows, hashed contact details
Meta Platforms (Ads)	Ireland, United States	Ads conversion reporting, only where connected by the Customer	Hashed contact details, conversion events
Apple	United States	Push notifications to the Subcontext iOS and Mac apps	Device tokens, notification content
Google Firebase	United States	Push notifications and crash reporting for the Subcontext Android app	Device tokens, notification content, crash diagnostics

3. Where Data Is Processed

- Customer data is stored in the AWS Ireland (eu-west-1) region
- Text conversations with AI agents are processed by AWS Bedrock in the EU (requests go to Ireland and may be served from another AWS EU region) and London. Requests to AI models routed to the United States are refused
- Voice calls use OpenAI and ElevenLabs in the United States, and only for customers who use voice
- AWS Bedrock does not store or train on prompts and responses. OpenAI does not train on API data, and may retain it for up to 30 days for abuse monitoring

4. How Sub-Processors Are Chosen

Every sub-processor is assessed before it is engaged, under the Supplier Risk Management Policy. The assessment covers:

- Security assurance, such as ISO 27001 certification or SOC 2 reports
- Data protection terms meeting Article 28 of the UK GDPR
- Where data is stored and processed, and the transfer safeguards in place
- For AI providers, whether customer data is retained, and confirmation that it is not used to train models
- Financial standing and service resilience

Each sub-processor is bound by a written agreement that includes confidentiality and security obligations, prompt notification of personal data breaches, and flow-down of equivalent obligations to its own sub-processors. Only the data a sub-processor needs for its task is sent to it.

5. Transfer Safeguards

Where data is transferred outside the United Kingdom, appropriate safeguards are in place in accordance with Chapter V of the UK GDPR, including the UK International Data Transfer Agreement (IDTA) and/or the EU Standard Contractual Clauses with the UK Addendum.

Where a US recipient is certified under the UK Extension to the EU-US Data Privacy Framework, transfers may also rely on the UK-US data bridge. The risks of transfers to the United States, and the measures that address them, are set out in the Transfer Risk Assessment.

6. Changes to Sub-Processors

Customers are notified at least 30 days before any new sub-processor is engaged, in accordance with the Data Processing Agreement.

When a sub-processor is added or replaced:

1. The new sub-processor is assessed under the Supplier Risk Management Policy, and the Transfer Risk Assessment and Data Protection Impact Assessment are updated where needed
2. Customers are notified at least 30 days before the new sub-processor is engaged, by email to the customer's account contacts
3. This list is updated, with its review date
4. Where a sub-processor is removed, its access is revoked, credentials are rotated, and deletion or return of the data is confirmed

7. Objections

A customer may object to a new sub-processor on reasonable data protection grounds by writing to hello@subcontext.com within the notice period. Subcontext will discuss the objection with the customer in good faith and, where possible, offer an alternative, such as not enabling the feature that relies on that sub-processor for the customer. Where no reasonable solution can be found, the customer's options are those set out in the Data Processing Agreement.

8. Customer-Connected Services

Customers can connect their own systems and accounts to the platform, such as their own policy administration or CRM systems, through custom integrations they configure. Those services are chosen by the customer and act under the customer's own agreements with them, so they are not Subcontext's sub-processors and do not appear on this list. Credentials for these connections are encrypted in the application, and calls to and from them are logged for 90 days.

9. Last Updated

This list was last reviewed on 1 October 2026.

It is reviewed at least annually, and whenever a sub-processor is added, removed or changes the location or purpose of its processing.

10. Related Documents

- Supplier Risk Management Policy
- Transfer Risk Assessment
- Data Protection Impact Assessment
- Data Retention & Deletion Policy

- Exit Plan & Data Return Policy

11. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors of Subcontext Ltd
Review	At least annually, and whenever a sub-processor changes
Effective	October 2026

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.