CARNO AI

Subprocessor Register

Approved third-party providers that may process client personal data when Carno AI acts as a processor.

Document owner	Carno AI	**Version**	1.0
Effective date	29 August 2026	**Review cycle**	At least annually and on material change

Purpose

This register identifies the subprocessors Carno AI has approved for use in delivering client automation services where Carno AI processes personal data on behalf of a client. It is intended to support transparency, vendor governance and Carno AI's contractual obligations as a processor under UK data protection law.

Scope. This is not a list of every software product used by Carno AI. A provider belongs in this register where Carno AI may cause that provider to process client personal data as part of a client service. Client-owned systems remain part of the client's own environment unless Carno AI independently introduces them into the processing chain.

Operating principles

Principle	Carno AI standard
Data minimisation	Only the personal data reasonably necessary for the relevant workflow or AI task should be processed.
API-first AI processing	Production client workflows should use controlled commercial/API environments rather than persistent consumer AI chats.
Client-system preference	Client data should remain in client-controlled systems where practical; Carno AI should avoid creating unnecessary permanent copies.
Higher-risk review	Identity documents, financial information, special-category data, profiling and significant automated decisions require separate assessment before use.
Change control	New subprocessors and material changes to existing providers should be assessed and recorded before use with client personal data.

Approved subprocessors

The entries below reflect Carno AI's currently approved core infrastructure and AI providers.

Provider	Purpose	Data potentially processed	Location / transfers	Safeguards & status
Hostinger International Ltd.	UK VPS infrastructure hosting for Carno AI's self-hosted n8n automation environment.	Workflow-specific client personal data passing through n8n, such as names, contact details, enquiry content, property and maintenance information.	Primary Carno AI VPS: United Kingdom. International processing may occur through Hostinger's underlying subprocessors where applicable.	**Approved.** Hostinger DPA; UK international-transfer provisions where applicable. Carno AI remains responsible for securing its VPS configuration.
OpenAI	AI-assisted classification, extraction, drafting, summarisation and other approved workflow processing through the OpenAI API.	Minimum necessary client text or fields required for the specific AI operation. Unnecessary identifiers and full records should not be sent.	Processing may occur in the UK and internationally depending on OpenAI infrastructure and subprocessors.	**Approved with controls.** OpenAI DPA; applicable SCCs and UK Addendum. API data is not used for model training by default. Certain abuse-monitoring data may be retained for up to 30 days under applicable controls.
Anthropic	AI-assisted classification, extraction, drafting, summarisation and other approved workflow processing through the Claude API / Developer Platform.	Minimum necessary client data required for the specific AI operation. Higher-risk or sensitive data requires separate assessment.	International processing may occur through Anthropic and its cloud infrastructure providers.	**Approved with controls.** Anthropic commercial DPA and applicable transfer mechanisms. Commercial/API use only for client workflows; apply data minimisation and do not enable optional data-sharing/training features for client-data projects.

Approval conditions

Approval does not mean that every provider should be used in every workflow. Carno AI should determine which providers are actually required for each client system and disclose relevant subprocessors through the applicable contractual process.

Where OpenAI or Anthropic is used, Carno AI should minimise prompt context and avoid sending personal identifiers where the AI task does not require them. Processing involving identity documents, bank details, special-category data, high-impact profiling or significant automated decisions should be escalated for a specific privacy and security assessment before production deployment.

Governance & change management

Subprocessor onboarding

Before a new provider is permitted to process client personal data, Carno AI should assess the provider's role, purpose, data categories, security posture, contractual data-processing terms, retention, processing locations, international-transfer safeguards and underlying subprocessors where relevant.

Client authorisation and notification

Carno AI's client Data Processing Agreement should define how subprocessor authorisation works. Where general written authorisation is used, Carno AI should provide appropriate notice of intended additions or replacements and allow the client an opportunity to object in accordance with the agreed terms.

Review triggers

This register should be reviewed at least annually and sooner where there is a material change to a provider's DPA, retention practices, processing locations, subprocessor list, security posture, Carno AI architecture or the categories of client data being processed.

Removal

A provider should be removed from approved use for client personal data where Carno AI no longer uses the service, cannot maintain appropriate contractual or security safeguards, or determines that the provider is no longer appropriate for the intended processing.

Official provider references

Reference	Official source
Hostinger Data Processing Addendum	hostinger.com/legal/dpa
OpenAI Data Processing Addendum	openai.com/policies/data-processing-addendum
OpenAI Subprocessor List	openai.com/policies/sub-processor-list
OpenAI API Data Controls	platform.openai.com/docs/guides/your-data
Anthropic DPA information	privacy.anthropic.com
Anthropic Trust Center / subprocessors	trust.anthropic.com

Document note

This register is an operational compliance document and does not constitute legal advice. It should be used alongside Carno AI's client DPA, information security controls, retention/deletion procedures and system-specific risk assessments. Material or higher-risk client processing should be reviewed against the exact facts and current UK requirements.