CARNO AI

Security & Privacy Overview

How Carno AI protects client data when building and operating business automation systems

Carno AI builds internal automation and AI-enabled workflows that connect with a client's existing business systems. Security and privacy are designed into those workflows from the start, with the aim of processing only the information required to deliver the agreed outcome.

Minimise data Only use the information a workflow genuinely needs.	**Separate clients** Separate workflows and credentials for each client.
Protect access Strong authentication, protected credentials and restricted infrastructure access.	**Control retention** Short operational retention and documented deletion/offboarding processes.

1. Our role with client data

For most client automation projects, the client remains the **data controller**: it decides why its Personal Data is used and what the business process is intended to achieve. Carno AI normally acts as a **data processor**, handling that information only to build, operate and support the agreed workflow and in accordance with the client's documented instructions.

These responsibilities are supported by a Client Data Processing Agreement (DPA), documented subprocessors and client-specific processing records. Higher-risk projects receive additional privacy/risk assessment before production deployment.

2. Security by design

Carno AI uses a risk-based security approach designed around confidentiality, integrity and availability. UK GDPR does not prescribe one universal technical configuration; organisations are expected to implement measures appropriate to the data, processing and risks involved. Carno therefore reviews controls in the context of each workflow rather than treating security as a one-time checklist.

3. Infrastructure and access protection

Control	Current Carno approach
Workflow infrastructure	Carno's primary self-hosted n8n automation infrastructure is hosted on a UK VPS.
Encrypted connections	Production services use HTTPS/encrypted transmission where appropriate. The n8n application port is not intended to be exposed directly to the public internet.
Network exposure	External firewall controls and a restricted service footprint are used to reduce unnecessary public access.
Administrative access	Administrative access is restricted. SSH key authentication is the production standard for server access, with stronger account authentication/MFA used where supported.
Credentials	Client API keys, OAuth connections and other credentials are kept in protected credential/configuration facilities rather than embedded into ordinary workflow content.
Client separation	Each client receives separate workflows and separate credentials even where the underlying automation pattern is similar.
Software hardening	Unnecessary n8n capabilities and public-facing features are disabled or restricted where appropriate, and community packages are not enabled by default.

4. Data minimisation and AI

Carno AI does not treat an AI model as a destination for an entire client database. Where an AI API is useful, the workflow should send only the information needed for the specific task. Unnecessary identifiers, documents and sensitive fields should be excluded wherever practicable.

Carno currently assesses OpenAI and Anthropic as AI/API subprocessors where their APIs are used for client processing. Client workflows are designed to use commercial/API environments, and Carno does not intentionally opt client-data projects into model-training or data-sharing programmes. Provider terms and data controls remain subject to periodic review.

For workflows involving identity documents, detailed financial information, special-category data, profiling, significant automated decisions or other higher-risk processing, Carno performs additional assessment and may require a DPIA, additional safeguards or a reduced automation scope before proceeding.

5. Retention and deletion

Carno aims to avoid creating unnecessary permanent copies of client information. Operational workflow data is retained only for the period reasonably needed for operation, troubleshooting, security and agreed support.

Carno's standard n8n execution-data target is a maximum age of **14 days**, with a maximum execution-count setting of **10,000**. Temporary exports, downloads and test files should be deleted promptly when no longer needed. At the end of an engagement, Carno follows a documented offboarding process to disable workflows, revoke credentials, return information where requested and delete operational client data subject to lawful retention requirements and protected backup cycles.

6. Backups, resilience and recovery

Carno maintains backup and recovery arrangements appropriate to its infrastructure and reviews these as the production environment changes. Backups are intended for resilience and recovery rather than as an alternative long-term archive. Where deleted information remains temporarily in protected backups, it is kept beyond ordinary use until removed through the applicable backup cycle.

7. Security incidents

Carno maintains a documented Personal Data Breach & Incident Response Procedure. Suspected incidents are logged, contained and assessed promptly. Where Carno acts as a processor and becomes aware of a Personal Data Breach affecting client data, the relevant client/controller is notified without undue delay and receives material updates as the investigation develops.

Incident handling includes credential revocation/rotation where appropriate, preservation of relevant evidence, risk assessment, remediation and a post-incident review for material events.

8. Subprocessors and international processing

Carno maintains a Subprocessor Register for providers that may process client Personal Data on Carno's behalf. Current assessed core providers include **Hostinger International Ltd.** for VPS infrastructure and **OpenAI** and **Anthropic** where their APIs are selected for a workflow.

Although Carno's primary VPS is hosted in the UK, Carno operates as an Australian business. Where a UK client makes Personal Data accessible to Carno in Australia and the transfer is a restricted transfer under UK GDPR, Carno's contractual framework anticipates an appropriate safeguard such as the UK IDTA or UK Addendum together with the required transfer assessment/data protection test. International-transfer arrangements are assessed per engagement where applicable.

9. Privacy governance

Governance measure	What it means for clients
Data Processing Agreement	Defines Carno's processor obligations, confidentiality, security, subprocessors, breach assistance, deletion/return, audits and transfers.
Subprocessor Register	Documents providers used in client processing and their role.
Information Security Policy	Defines Carno's internal security baseline and responsibilities.
Retention & Deletion Policy	Defines standard retention and deletion expectations.
Incident Response Procedure	Provides a repeatable response and client-notification process for security incidents/personal-data breaches.
Offboarding Procedure	Controls workflow shutdown, credential revocation, data return/deletion and completion evidence.
ROPA / Data-Flow Register	Records Carno's processing activities and client-specific processing/data flows.
DPIA process	Screens new Personal Data workflows and provides a full assessment process for likely high-risk processing.

10. Human oversight and automation risk

Carno's objective is to remove repetitive administration without unnecessarily removing human judgement. Where an automation produces an uncertain result, handles an exception or could materially affect an individual, the workflow can be designed to escalate to a person rather than make an uncontrolled decision.

Carno's standard position is to avoid solely automated decisions with legal or similarly significant effects unless the specific use case has been assessed, the client has a lawful basis and appropriate safeguards are in place.

11. What Carno expects from clients

Security is shared across the overall system. Clients remain responsible for the security, permissions and lawful use of their own systems and for ensuring Carno receives appropriate access and instructions. Carno encourages clients to provide the minimum access required, promptly remove obsolete accounts/credentials, identify sensitive or higher-risk data during scoping and notify Carno of relevant security or privacy requirements.

12. Security reviews and assurance

Carno reviews its controls as its infrastructure, client base and risk profile develop. Security measures may be improved or replaced as technology and threats change. Carno's current compliance foundation includes documented security, privacy, incident, retention, offboarding, transfer and DPIA processes.

Carno does **not** currently claim ISO 27001 certification, Cyber Essentials certification, formal UK GDPR certification or any other security certification that has not actually been obtained. Future certifications may be pursued as the business matures.

13. Requesting further information

Clients and prospective clients can request relevant security/privacy information during due diligence. Where appropriate, Carno can provide its DPA, current Subprocessor Register and additional policy information, subject to confidentiality and security considerations.

Privacy & security contact: admin@carnoai.com
Website: carnoai.com

Important note

This overview is intended to explain Carno AI's current security and privacy approach in a clear client-facing format. It does not replace the applicable service agreement, DPA, client instructions or a project-specific risk assessment. Specific technical controls and subprocessors may differ where a client engagement requires a different architecture, in which case those differences should be documented and agreed.

Reference basis

This overview has been prepared with reference to current ICO guidance on the UK GDPR security principle and Article 32. The ICO describes a risk-based approach requiring appropriate technical and organisational measures and highlights confidentiality, integrity, availability, resilience, restoration, testing, access control and encryption/pseudonymisation where appropriate. ICO security guidance is currently under review following the Data (Use and Access) Act, so Carno should continue to review its controls and documentation as guidance changes.