

COMPLIANCE AUDIT REPORT

AI Data Privacy and Security

Prepared for: **Your Company**

Audit Reference: **JNVOY-11DE328B52C1**

Generated: **10 October 2026 at 19:11 UTC**

Period: **N/A to N/A**

Prepared by Jnvoy AI Privacy Firewall

jnvoy.onrender.com | github.com/Jeevan2191999/jnvoy

1. Compliance Statement

CONFIRMED: Zero sensitive data was transmitted to any LLM API during the audit period.

All requests routed through Jnvoy during the audit period were inspected for personally identifiable information (PII) before being forwarded to any large language model. Sensitive data identified in any request was redacted and replaced with reversible tokens prior to transmission. The original values were restored in the response before delivery to the end user. No raw PII was transmitted to any external LLM provider at any point during the audit period.

Statement	Value
Audit Reference	JNVOY-11DE328B52C1
Company	Your Company
Audit Period Start	N/A
Audit Period End	N/A
Report Generated	2026-10-10 19:11 UTC
Sensitive Data Transmitted to LLM	NO
Governing Standard	UK GDPR, Data Protection Act 2018, FCA AI Governance Guidelines

2. Executive Summary

During the audit period, Jnvoy processed 0 API requests on behalf of Your Company. Of these requests, 0 instances of personally identifiable information were detected and redacted before any data was forwarded to an external LLM provider. The semantic cache resolved 0.0% of requests without contacting any external provider, reducing both cost and data exposure.

Metric	Value	Notes
Total API calls processed	0	All requests inspected for PII
PII instances detected and redacted	0	None transmitted to any LLM
Cache hit rate	0.0%	Requests resolved without external call
Average request latency	0ms	Including PII detection overhead
Sensitive data transmitted	ZERO	Confirmed by audit log

3. PII Detection Breakdown

The following categories of personally identifiable information were detected and redacted during the audit period. All instances were replaced with reversible tokens before transmission and restored in the response. Raw values were never transmitted.

No PII was detected during the audit period.

4. Technical Methodology

PII Detection Engine

Jnvoy uses Microsoft Presidio, an enterprise-grade NLP-based PII detection engine, combined with pattern-based recognisers for UK-specific data types. Detection runs locally on Jnvoy infrastructure. No data is sent to any external service for the purpose of PII detection. The following entity types are supported: person names, email addresses, phone numbers, credit card numbers, IBAN codes, IP addresses, UK NHS numbers, National Insurance numbers, UK postcodes, sort codes, account numbers, passport numbers, API keys, and secret tokens.

Tokenisation and Restoration

When PII is detected, each instance is replaced with a unique reversible token before the request is forwarded to the LLM. The token map is held in memory for the duration of the request and is used to restore original values in the LLM response before delivery to the end user. The token map is never persisted. Only PII type counts and timestamps are written to the audit log.

Audit Logging

Every request is recorded in a PostgreSQL audit database with a unique audit ID, timestamp, PII type counts, provider used, model used, latency, and cache status. Raw PII values are never written to the audit log. Only hashes and type counts are stored.

This report was automatically generated by Jnvoy AI Privacy Firewall on 10 October 2026. Audit Reference: JNVOY-11DE328B52C1.

Jnvoy is open source software. Source code available at github.com/Jeevan2191999/jnvoy. This report does not constitute legal advice.