CallQ

Data Protection Officer Briefing Document

A comprehensive guide to how CallQ processes, protects, and manages call transcript data — written specifically for Data Protection Officers and compliance leads at UK law firms.

Platform	CallQ — AI-powered call quality analysis for UK law firms
Operator	Standard Consulting and Training Ltd
Role	Data Processor (your firm is the Data Controller)
Data types	Call transcripts (may contain special category data under UK GDPR)
Data storage	EU-hosted database (Supabase). Transcripts and analyses do not leave the EU.
AI provider	Anthropic Claude API (closed model, no training on customer data)
PII redaction	On by default. Personal identifiers stripped before AI analysis.
Contact	david@revueiq.com
Security details	cal-iq.com/safety

Document version: 1.0 — March 2026

This document is provided to assist your firm's data protection assessment. It is not legal advice. We recommend your DPO reviews this alongside CallQ's Terms of Service, Privacy Policy, and Data Processing Agreement.

Contents

1. Purpose of This Document

This document is designed to give your firm's Data Protection Officer (or the person responsible for data protection) the information needed to assess whether CallQ is appropriate for use within your firm.

It addresses the specific questions that the Law Society's GDPR guidance for solicitors says firms should ask when engaging a data processor. It covers the technical safeguards, the contractual framework, the data flows, and the specific considerations around special category data and AI processing.

After reading this document, your DPO should have sufficient information to complete a Data Protection Impact Assessment for CallQ's use within your firm. A DPIA template is available on request from david@revueiq.com.

2. What CallQ Does

CallQ is a software-as-a-service platform that analyses call transcripts for UK law firms. Your firm uploads transcripts of phone calls with clients. CallQ's AI analyses each transcript against eight quality dimensions designed for legal client interactions and returns:

- A composite quality score out of 100
- Individual scores across eight dimensions (e.g. empathy, compliance, active listening)
- Automatic call classification (type, department, urgency, outcome)
- Vulnerability detection aligned with the FCA's four-driver model
- Handler performance tracking
- Sentiment analysis showing how the caller's emotional state changed during the call
- Specific strengths, areas for improvement, and actionable recommendations

CallQ does not record, intercept, or access live phone calls. It only processes text transcripts that your firm has already created and chooses to upload.

3. Data Processing Roles: Controller and Processor

> **Key point**
>
> Your firm is the Data Controller. CallQ (Standard Consulting and Training Ltd) is the Data Processor. CallQ processes personal data within call transcripts solely on your firm's instructions, for the sole purpose of providing the analysis service.

This is consistent with the Law Society's GDPR guidance, which states that solicitors are typically data controllers of their clients' personal data, and that service providers processing data on their behalf are processors.

CallQ does not determine the purposes or means of processing. Your firm decides which transcripts to upload, which users have access, and how the analysis is used. CallQ processes the data as instructed and returns the results.

A Data Processing Agreement (DPA) is provided to every customer, setting out the terms under Article 28 UK GDPR. This is available before any data is uploaded.

4. What Data CallQ Processes

4.1 Data provided by your firm (transcripts)

- Call transcript text (the words spoken during a phone call)
- Optional metadata: call date, handler name, department, call duration
- Transcripts are uploaded by your firm's authorised users via the web interface

4.2 Account data

- User names, email addresses, job titles
- Firm name, SRA number, website URL
- Usage data: analyses completed, last login, features used

4.3 Data CallQ generates

- Quality scores, classifications, vulnerability flags, and recommendations
- Aggregated dashboard data, handler performance metrics, trend analysis
- These are derivative outputs generated from the transcripts your firm provides

5. Special Category Data

> **Important**
> Call transcripts from law firms are likely to contain special category data under Article 9 UK GDPR. CallQ is designed with this classification in mind.

Call transcripts may contain:

- **Health information** — callers describing injuries, medical conditions, mental health
- **Details of legal proceedings** — the nature of claims, case circumstances
- **Vulnerability indicators** — financial distress, bereavement, domestic abuse, cognitive difficulties
- **Potentially:** racial or ethnic origin, sexual orientation, trade union membership, religious beliefs (depending on call content)

CallQ's security architecture, PII redaction, closed AI model, data isolation, and retention policies are specifically designed for this level of data sensitivity. The safeguards described in this document reflect the fact that we are handling data at the highest classification level.

Your firm should ensure that its call recording consent notices and privacy notices cover AI-powered analysis as a processing purpose. CallQ provides template privacy notice wording to assist with this.

6. PII Redaction: On by Default

> **Key safeguard**
>
> CallQ automatically redacts personally identifiable information from every transcript before it is sent to the AI for analysis. This is on by default for every firm. The AI never sees who your callers are. It only sees the conversation.

Before any transcript reaches the Anthropic Claude API for analysis, CallQ's PII redaction engine removes:

- Phone numbers
- Addresses
- NHS numbers

This is a deliberate design decision. Call quality scoring is based on how a conversation was handled — the empathy, the listening, the information gathering, the compliance. None of that requires knowing the caller's identity.

By stripping personal identifiers before they reach the AI provider, CallQ significantly reduces the sensitivity of the data being processed externally. The AI receives a conversation transcript with personal identifiers removed. It returns a quality analysis. At no point does the AI model know who the caller was.

This approach directly supports the data minimisation principle under UK GDPR: only the data necessary for the processing purpose is shared with the sub-processor.

PII redaction settings can be adjusted in the firm's account settings. We recommend keeping redaction on — it simplifies your data protection position and reduces risk.

7. How AI Analysis Works

CallQ uses the Anthropic Claude API to analyse transcripts. This section explains how the AI processing works, because this is likely to be the area of most scrutiny for your DPO.

7.1 The closed model

The Anthropic Claude API is a closed model. Anthropic's API terms explicitly state that customer prompts and completions are not used for model training. This is materially different from consumer-facing AI tools (such as ChatGPT's free tier) where user inputs may contribute to training data.

7.2 What is sent to the API

For each transcript, CallQ sends the PII-redacted transcript text and a structured system prompt (which defines the scoring framework and expected output format) to the API. The API returns a structured JSON response containing scores, classifications, flags, and narrative commentary. This response is stored in CallQ's database.

7.3 Data retention by Anthropic

Anthropic retains API inputs for a limited period for abuse and safety monitoring purposes only. Inputs are not stored permanently and are not used for any purpose other than safety monitoring. Anthropic's API Data Processing Agreement provides the contractual terms for this processing.

7.4 No human review

Transcripts processed through the API are not reviewed by Anthropic employees unless required for safety or legal compliance purposes. Under normal operation, the processing is entirely automated.

8. Data Flow Architecture

The following diagram shows how data moves through CallQ, from upload to dashboard:

Stage	What happens	Where
1. Upload	User pastes or uploads transcript via web interface	Vercel (web hosting)
2. Storage	Raw transcript stored in encrypted database	Supabase (PostgreSQL, EU)
3. PII redaction	Personal identifiers stripped from transcript	CallQ server
4. AI analysis	PII-redacted transcript sent to Claude API; structured analysis returned	Anthropic API (US)
5. Results storage	Analysis results stored alongside original transcript	Supabase (PostgreSQL, EU)
6. Presentation	Dashboard renders scores, charts, reports for authorised users	Vercel (web hosting)

Key point

PII redaction occurs at Stage 3, before the transcript reaches the AI at Stage 4. The AI provider never receives personal identifiers. The raw transcript (with PII) is stored only in CallQ's encrypted database on EU servers, accessible only to your firm's authorised users.

9. Sub-Processors

The Law Society's GDPR guidance states that firms must check what restrictions are in place to prevent data being shared with subcontractors, and whether those subcontractors are also GDPR-compliant. Here is every third-party service that touches your data:

Sub-processor	Purpose	Location	Receives transcripts?
Anthropic, PBC	AI transcript analysis	United States	Yes — PII-redacted only. Not used for training.
Supabase, Inc	Database hosting and authentication	European Union	Yes — stores all data on EU servers. AES-256 encryption at rest.
Vercel, Inc	Web application hosting	US + global edge	No — serves the application. May log IP addresses.
Stripe, Inc	Payment processing	United States	No — billing details only. PCI DSS compliant.
HubSpot, Inc	Marketing email automation	United States	No — email address, firm name, usage metrics only.

CallQ will notify your firm at least 30 days before adding or replacing any sub-processor. Your firm has the right to object to a new sub-processor. If the objection cannot be resolved, your firm may terminate the agreement.

CallQ remains fully liable for the acts and omissions of its sub-processors.

10. Security Architecture

CallQ's security architecture is designed for the sensitivity of legal sector data, including special category data.

Control	Implementation
Encryption at rest	AES-256 managed encryption via Supabase for all stored data. Database hosted on EU servers.
Encryption in transit	TLS 1.3 for all communications between browser, server, and AI API.
Row-level security	PostgreSQL database-level isolation ensures each firm's data is completely separated. Enforced at infrastructure level, not application level.
PII redaction	On by default. Personal identifiers stripped before AI analysis. The AI never sees caller identity.
Role-based access	Four permission levels: Admin, Manager, Analyst, Viewer. Handler performance data restricted to management roles.

Authentication	Email/password with optional multi-factor authentication. Session tokens with configurable expiry.
Audit trail	All data access, analysis events, and user actions logged with timestamp and user identity. Immutable audit log.
API security	Rate limiting, input validation via structured schemas (Zod), CORS restrictions.
Closed AI model	Anthropic API does not use customer data for model training. Limited retention for safety monitoring only.

11. Data Retention and Deletion

Scenario	Retention period	What happens
Active subscription	Duration of subscription	All data accessible to authorised users.
Subscription cancelled	60 days post-cancellation	Read-only access for export. After 60 days, all transcripts and analyses permanently deleted.
Trial expired (no conversion)	90 days post-expiry	Read-only access. After 90 days, permanently deleted.
Data deletion request	Upon request	All firm data permanently deleted. Written confirmation provided.
Payment records	7 years	Retained per HMRC requirements. Processed by Stripe.
Backup copies	30 days after primary deletion	Purged from all backup systems.

Your firm can export all data at any time via the dashboard's PDF report and CSV export functions. Data portability is built into the platform.

12. International Data Transfers

Several sub-processors are based in the United States. However, CallIQ's database — which holds all transcripts, analyses, and firm data — is hosted by Supabase on EU servers. This means your firm's stored data does not leave the European Union.

The primary international transfer is the PII-redacted transcript data sent to Anthropic's Claude API in the United States for AI analysis. Because PII redaction is applied before this transfer, the data reaching Anthropic contains no personal identifiers. The AI processes the redacted transcript and returns the analysis results, which are then stored on the EU-hosted database.

Other US-based sub-processors (Vercel, Stripe, HubSpot) do not receive transcript data. Vercel serves the web application and may log IP addresses. Stripe processes billing details only. HubSpot holds email addresses and firm names for marketing communications only.

The appropriate transfer mechanism for each US-based sub-processor should be confirmed by your firm's DPO. The available mechanisms include:

- The UK-US Data Bridge (extension to the EU-US Data Privacy Framework)
- The UK International Data Transfer Agreement (UK IDTA)
- The UK Addendum to EU Standard Contractual Clauses
- Standard Contractual Clauses (SCCs) with supplementary measures

For your DPO

Your firm's stored data (transcripts, analyses, user accounts) is held on EU servers via Supabase. The only international transfer involving transcript content is to Anthropic for AI analysis — and that data is PII-redacted before transfer, containing no personal identifiers. This significantly reduces the risk profile. Your DPO should review Anthropic's API Data Processing Agreement to confirm the specific safeguards. A copy can be requested from david@revueiq.com.

13. Law Society GDPR Guidance: Point-by-Point Compliance

The Law Society's GDPR guidance for solicitors sets out specific checks firms should make when engaging a data processor. This section maps each requirement directly to CallQ's safeguards.

Law Society requirement	How CallQ meets it
Clear written contract setting out what the processor does with data	Data Processing Agreement provided to every customer before any data is uploaded. Specifies scope, data types, security measures, breach notification, sub-processors, and deletion terms.
Processor prohibited from using data for own purposes	CallQ processes transcripts solely to provide the analysis service. We do not sell, licence, or use your data for any other purpose. Stated in ToS and DPA.
Security measures including encryption	PII redaction on by default. AES-256 encryption at rest. TLS 1.3 in transit. Row-level database security. Role-based access. Immutable audit trail. Closed AI model.
Restrictions on sharing with subcontractors	All sub-processors named in DPA. Only Anthropic and Supabase receive transcript data (Anthropic receives PII-redacted transcripts only). 30-day notice before changes. Right to object.
Sub-contractor GDPR compliance	Each sub-processor operates under its own data processing terms. Anthropic: closed model, no training use, limited retention. Supabase: EU-hosted, managed encryption, database-level security.
Data minimisation	Only transcript data uploaded by the firm is processed. PII redaction ensures the AI receives only what is necessary for quality scoring. No data collected beyond service requirements.
Storage limitation	Defined retention periods: active subscription, 60-day post-cancellation, 90-day post-trial. Permanent deletion after retention. Backup purge within 30 days.
Accountability	Full audit trail. DPIA template provided. DPA with audit rights. This briefing document. Security details published at cal-iq.com/safety.

14. Data Subject Rights

As the data controller, your firm is responsible for responding to data subject access requests and other rights requests relating to the personal data within call transcripts. CallQ supports these rights as follows:

- **Right of access:** Your firm's authorised users can access all transcripts and analyses via the dashboard. PDF and CSV export is available for portability.
- **Right to rectification:** Transcript data can be corrected by your firm's administrators.
- **Right to erasure:** Your firm can request deletion of specific transcripts or all firm data. CallQ will action deletion requests and provide written confirmation.

- **Right to restrict processing:** CallQ will comply with any restriction request relayed by your firm.
- **Right to data portability:** PDF report and CSV export built into the platform.
- **Right to object:** Your firm controls what data is uploaded. No data is processed without your firm's active instruction.

15. Data Protection Impact Assessment

Given that CallQ processes special category data using new technology (AI), a DPIA is likely required under Article 35 UK GDPR before your firm begins using the platform.

CallQ provides a DPIA template to help your DPO complete this assessment. The template covers:

- Description of the processing (what data, why, how)
- Lawful basis guidance (likely legitimate interest for quality monitoring, or contract performance)
- Necessity and proportionality assessment
- Risk assessment specific to AI processing and international transfers
- Mitigations provided by CallQ (PII redaction, closed model, encryption, isolation, retention)
- Whether existing call recording consent notices cover AI analysis

Request the DPIA template from david@revueiq.com.

16. Breach Notification

In the event of a personal data breach affecting your firm's data, CallQ will:

- Notify your firm without undue delay and in any event within 72 hours of becoming aware of the breach
- Provide details of: the nature of the breach, categories and approximate number of data subjects affected, likely consequences, and measures taken or proposed
- Cooperate fully with your firm's breach response and ICO notification obligations

This is set out in the Data Processing Agreement.

17. Contractual Documentation Available

The following documents are available to support your firm's data protection assessment:

Document	Purpose	How to access
Terms of Service	Governs the contractual relationship, liability, acceptable use	Available on request from david@revueiq.com
Privacy Policy	How CallQ collects and processes user personal data	Available on request from david@revueiq.com

Data Processing Agreement	Article 28 DPA covering processor obligations, sub-processors, security, breach notification, deletion	Available on request from david@revueiq.com
DPIA Template	Template to help your DPO complete a data protection impact assessment	Available on request from david@revueiq.com
This Briefing Document	Comprehensive overview for DPO assessment	cal-iq.com/safety

18. Recommended Actions for Your Firm

To use CallQ in a way that is compliant with UK GDPR and consistent with the Law Society's guidance, we recommend your firm takes the following steps:

1. Review this document

Ensure your DPO has read this briefing and is satisfied with the safeguards described.

2. Complete a DPIA

Use the CallQ DPIA template (available on request) to formally assess the data protection implications for your firm.

3. Review your call recording consent notices

Ensure your existing privacy notices and call recording disclosures cover AI-powered analysis as a processing purpose. CallQ provides template wording to assist.

4. Review the Data Processing Agreement

Request the DPA from david@revueiq.com. Review it with your DPO. Sign it before uploading any client data.

5. Confirm international transfer mechanisms

Your DPO should confirm the appropriate transfer mechanism for each US-based sub-processor (Anthropic, Vercel, Stripe, HubSpot). Note that Supabase hosts CallQ data on EU servers, so no international transfer mechanism is required for the database.

6. Configure user permissions

Set up role-based access within CallQ so that handler performance data is restricted to appropriate management roles.

7. Verify PII redaction is on

PII redaction is on by default. Confirm it remains enabled in your firm's account settings.

8. Begin with a controlled trial

Upload a small number of transcripts initially to verify the analysis quality and confirm you are comfortable with the data handling before scaling.

If you have any questions about the information in this document, or if your DPO requires additional detail on any aspect of CallQ's data handling, please contact:

David Standard

Standard Consulting and Training Ltd

david@revueiq.com

cal-iq.com/safety