# CallQ

## Data Protection Impact Assessment Template

This template is designed to help your firm's Data Protection Officer complete a DPIA for the use of CallQ within your firm. Grey fields contain CallQ's pre-populated information. White fields are interactive — click to type directly into this PDF.

### Assessment details

**Firm name:**

**DPO / assessor:**

**Date of assessment:**

**Review date:**

| | |
|---|---|
| System assessed | CallQ — AI-powered call quality analysis (cal-iq.com) |
| Data controller | [Your firm — entered above] |
| Data processor | Standard Consulting and Training Ltd (CallQ) |

**How to use this template**

Grey fields are pre-populated with CallQ information and cannot be edited. White fields with a border are interactive form fields — click on them and type directly in Adobe Acrobat or your PDF reader. Tick boxes are clickable. Save the completed PDF as part of your firm's data protection records. Review annually or when processing changes significantly.

Document version: 1.0 — March 2026

# 1. Description of the Processing

## 1.1 What is the nature of the processing?

**Nature of processing (pre-populated)**

CallQ is a software-as-a-service platform that analyses call transcripts from law firm telephone conversations using AI (Anthropic Claude API). The firm uploads text transcripts of client calls. CallQ's AI analyses each transcript against eight quality dimensions designed for legal client interactions, detects caller vulnerability using FCA-aligned criteria, classifies calls by type, department, and urgency, and returns structured quality scores, recommendations, and management intelligence via an interactive dashboard.

## 1.2 What is the scope of the processing?

**Scope of processing (pre-populated)**

The processing covers call transcripts uploaded by the firm's authorised users. This includes the text content of phone conversations between the firm's call handlers and callers (clients, potential clients, and third parties). The firm controls which transcripts are uploaded and how many. The free trial includes 100 analyses. Paid subscriptions range from 200 to 5,000+ calls per month depending on tier.

## 1.3 What is the context of the processing?

> *Your firm must complete this field. Consider: What is the relationship between your firm and the callers? Are callers aware their calls are recorded? Does your existing call recording notice cover AI analysis?*

**Describe the context within your firm**

*Consider: your firm's relationship with callers, existing call recording practices, consent notices*

## 1.4 What are the purposes of the processing?

**Purposes (pre-populated)**

The purposes are: (a) monitoring and improving the quality of client call handling across the firm; (b) detecting caller vulnerability to ensure appropriate handling and compliance with regulatory expectations; (c) tracking handler performance to identify training needs and evidence improvement; (d) providing management intelligence on call quality trends, patterns, and operational issues; (e) evidencing the firm's commitment to client service standards and regulatory compliance.

> *Confirm these purposes align with your intended use. Add any additional purposes below.*

**Additional purposes specific to your firm (if any)**

# 2. Lawful Basis for Processing

## 2.1 Lawful basis under Article 6 UK GDPR

**Lawful basis options (pre-populated)**

Article 6(1)(f) — Legitimate interests: The firm has a legitimate interest in monitoring call quality, ensuring regulatory compliance, identifying vulnerability, and improving client service. This must be balanced against the rights of the data subjects. A Legitimate Interests Assessment should be documented separately.
Article 6(1)(b) — Contract performance: Where call quality monitoring is part of the firm's contractual obligations to clients.
Article 6(1)(c) — Legal obligation: Where the processing supports the firm's SRA regulatory obligations regarding service standards and vulnerable client handling.

*Your DPO should confirm which lawful basis applies. If relying on legitimate interests, complete a separate Legitimate Interests Assessment.*

**Lawful basis selected and justification**

## 2.2 Condition for processing special category data under Article 9

**Article 9 conditions (pre-populated)**

Call transcripts are likely to contain special category data including health information and vulnerability indicators.
Article 9(2)(g) — Substantial public interest: Processing is necessary for reasons of substantial public interest, on the basis of UK law (Data Protection Act 2018, Schedule 1).
Article 9(2)(f) — Legal claims: Processing is necessary for the establishment, exercise, or defence of legal claims.
Schedule 1, Part 2, Paragraph 6 — Statutory purposes: Processing necessary for compliance with regulatory requirements.

*This is a critical determination. If uncertain, seek specialist data protection legal advice.*

**Article 9 condition selected and justification**

# 3. Personal Data Involved

## 3.1 Categories of data subjects

**Data subjects (pre-populated)**

Callers: Clients, potential clients, and third parties (insurers, medical providers, other solicitors) whose calls are recorded and transcribed by the firm.
Call handlers: The firm's employees or agents who handle the calls.

## 3.2 Types of personal data

**Data types (pre-populated)**

Within transcripts (before PII redaction): Caller names, phone numbers, addresses, NHS numbers, health information, details of injuries or medical conditions, legal matter details, financial circumstances, vulnerability indicators, and potentially racial or ethnic origin, sexual orientation, trade union membership, or religious beliefs.
After PII redaction (what the AI receives): The conversation text with phone numbers, addresses, and NHS numbers removed. The AI does not receive personal identifiers.
Account data: User names, email addresses, job titles, firm name, SRA number.
Handler data: Handler names, department, call volume, quality scores.

## 3.3 Volume of data

> *Your firm should complete this based on your expected usage.*

**Estimated calls per week/month**

**Number of call handlers**

**Approximate number of callers affected**

# 4. Data Flows

## 4.1 How data is collected

> *CallQ does not record or transcribe calls. Your firm must describe how transcripts are created.*

**How are call transcripts created at your firm?**

*Phone system used, recording process, transcription method, caller notification*

## 4.2 How data flows through CallQ

**Data flow (pre-populated)**

1. The firm's authorised user uploads a call transcript via the CallQ web interface.
2. The raw transcript is stored in CallQ's encrypted database, hosted on EU servers (Supabase).
3. PII redaction is applied automatically — phone numbers, addresses, and NHS numbers are stripped.
4. The PII-redacted transcript is sent to the Anthropic Claude API (United States) for AI analysis. The AI does not receive personal identifiers.
5. The AI returns a structured analysis, stored in the EU-hosted database alongside the original transcript.
6. Authorised users view results via the CallQ dashboard. Data can be exported as PDF or CSV.

## 4.3 Sub-processors

| Sub-processor | Purpose | Location | Receives transcripts? |
|---|---|---|---|
| Anthropic, PBC | AI transcript analysis | United States | PII-redacted transcripts only. Closed model, not used for training. |
| Supabase, Inc | Database & auth | European Union | Yes — stores all data on EU servers. AES-256 encryption. |
| Vercel, Inc | App hosting | US + global edge | No — serves the app only. |
| Stripe, Inc | Payments | United States | No — billing details only. |
| HubSpot, Inc | Marketing emails | United States | No — email and firm name only. |

## 4.4 International transfers

**International transfer summary (pre-populated)**

All stored data (transcripts, analyses, firm accounts) is held on EU servers via Supabase. No international transfer mechanism is required for the database.
The primary international transfer is PII-redacted transcript data sent to Anthropic (US) for AI analysis. Personal identifiers are removed before this transfer.
Other US-based sub-processors (Vercel, Stripe, HubSpot) do not receive transcript data.

> *Your DPO should confirm the transfer mechanism for each US-based sub-processor. Options: UK-US Data Bridge, UK IDTA, UK Addendum to EU SCCs, or Standard Contractual Clauses.*

**Transfer mechanisms confirmed by DPO**

# 5. Necessity and Proportionality

## 5.1 Is the processing necessary?

**Necessity assessment (pre-populated)**

• Manual call monitoring covers fewer than 2% of calls at most firms. AI analysis enables monitoring of every call.
• Vulnerability detection at scale is not achievable through manual monitoring alone.
• Consistent, objective scoring requires a structured framework applied uniformly.
• Trend analysis and handler comparison require aggregated data across all calls, not a sample.

## 5.2 Is the processing proportionate?

**Proportionality assessment (pre-populated)**

• PII redaction removes personal identifiers before AI analysis, minimising data shared externally.
• The AI receives only the conversation content necessary for quality scoring — not the caller's identity.
• Data is stored on EU servers, reducing international transfer risk.
• The closed AI model does not use transcripts for training.
• Data retention is defined and limited.
• The firm controls what is uploaded and can delete data at any time.
• The processing serves a genuine regulatory and client welfare purpose.

## 5.3 Less intrusive alternatives considered

**Alternatives considered (pre-populated)**

• Manual call monitoring: Covers only 1–2% of calls. Does not scale. Misses vulnerability.
• Anonymised transcripts only: PII redaction is already applied. Full anonymisation would remove context needed for performance tracking.
• On-premise AI processing: Not available at viable cost or complexity for law firms.
• No monitoring: Leaves the firm unable to evidence quality or detect vulnerability.

> *Review and confirm the above. Add firm-specific considerations below.*

**Additional firm-specific necessity or proportionality considerations**

# 6. Risk Assessment

This section identifies risks to data subjects. Likelihood and severity are rated Low, Medium, or High. All mitigations are provided by CallQ unless otherwise stated.

| Risk | L | S | Mitigations | Residual |
|---|---|---|---|---|
| Unauthorised access to transcripts with sensitive data | Low | High | AES-256 at rest. TLS 1.3 in transit. Row-level database security. Role-based access (4 levels). Optional MFA. Audit trail. | Low |
| AI provider retains or misuses transcript data | Low | High | PII redaction before AI. Closed model — no training use. Limited retention for safety only. No human review. | Low |
| Data exposed via international transfer | Low | Med | Database on EU servers. Only PII-redacted data to Anthropic (US). Other US sub-processors receive no transcripts. | Low |
| Data breach at CallQ or sub-processor | Low | High | Encryption at rest and in transit. Database isolation. 72-hour breach notification. PII redaction limits exposure. | Low |
| Inaccurate AI analysis — unfair treatment of handlers | Med | Med | Management tool, not sole basis for decisions. Explicit guidance against sole-basis disciplinary action. | Low |
| Caller distress at AI analysis of their calls | Low | Med | Firm updates recording notices. Template wording provided. PII redaction means AI does not see caller identity. | Low |
| Handler distress at being scored by AI | Med | Med | Handler data restricted to management roles. Development tool, not surveillance. Anonymisation options. | Low |
| Vulnerability flags used inappropriately | Low | High | Assistive flag only, not clinical determination. Access controlled by permissions. Guidance provided. | Low |
| Data retained longer than necessary | Low | Low | 60-day post-cancellation, 90-day post-trial. Automatic deletion. On-demand deletion. Backups purged within 30 days. | Low |

> *Review risk ratings. Adjust if your circumstances differ. Add firm-specific risks below.*

**Additional firm-specific risks**

# 7. Consultation

## 7.1 Views of data subjects

> *Article 35(9) UK GDPR requires you to seek the views of data subjects or their representatives where appropriate. Consider: staff whose calls will be analysed, client representatives, trade unions or staff forums.*

**Have data subjects been consulted? If yes, summarise. If no, explain why.**

## 7.2 Internal stakeholders consulted

**Which internal stakeholders have been consulted?**

*E.g. managing partner, compliance partner, HR director, IT manager, client care manager*

# 8. Measures to Address Risks

## 8.1 Measures provided by CallQ

**CallQ safeguards (pre-populated)**

- PII redaction on by default — personal identifiers removed before AI analysis
- EU-hosted database — stored data does not leave the European Union
- Closed AI model — customer data not used for training
- AES-256 encryption at rest, TLS 1.3 in transit
- Row-level security — firm data isolated at database level
- Role-based access control (Admin, Manager, Analyst, Viewer)
- Immutable audit trail
- Defined data retention with automatic deletion
- Data Processing Agreement (Article 28 compliant)
- Breach notification within 72 hours
- PDF and CSV export for data portability
- Deletion on request with written confirmation

### 8.2 Measures your firm should implement

**Recommended measures (pre-populated)**

- Update call recording consent notices to cover AI analysis
- Update the firm's privacy notice to reference CallQ as a processor
- Inform call handlers that calls will be analysed by AI and explain the purpose
- Establish policy on use of CallQ scores (not sole basis for disciplinary action)
- Restrict CallQ access to authorised personnel with appropriate permission levels
- Review and sign the CallQ Data Processing Agreement
- Confirm international transfer mechanisms for US-based sub-processors
- Train relevant staff on CallQ purpose and appropriate use of vulnerability flags
- Schedule annual review of this DPIA

> *Confirm which measures your firm will implement. Add additional measures below.*

**Additional measures your firm will take**

## 9. Overall Assessment and Decision

### 9.1 Summary of residual risk

**What is the overall level of residual risk after mitigations?**

### 9.2 Decision

> *If residual risk remains high after mitigations, Article 36 UK GDPR requires prior consultation with the ICO before proceeding.*

- ☐ Approved — residual risks are acceptable and appropriately mitigated
- ☐ Approved with conditions — additional measures required before processing begins
- ☐ Not approved — residual risks too high, refer to ICO under Article 36

**Conditions or additional measures (if applicable)**

### 9.3 Sign-off

**DPO / Assessor**

**Name:**

**Role:**

**Date:**

**Approved by (senior partner / COLP)**

**Name:**

**Role:**

**Date:**

## 10. Review Schedule

This DPIA should be reviewed:

- Annually from the date of initial assessment
- When there is a significant change to the processing
- When CallQ notifies a sub-processor change (30-day notice provided)
- If a data breach occurs involving CallQ
- If relevant legislation or regulatory guidance changes

**Review log**

**Review 1**
**Date:**

**Reviewed by:**

**Changes made and outcome**

**Review 2**
**Date:**

**Reviewed by:**

**Changes made and outcome**

**Review 3**

**Date:**

**Reviewed by:**

**Changes made and outcome**

**Review 4**
**Date:**

**Reviewed by:**

**Changes made and outcome**

---

If you have any questions about completing this DPIA, please contact:

**David Standard**
Standard Consulting and Training Ltd
david@revueiq.com
cal-iq.com/safety

CalIQ — Listening between the lines