PROOF Trust Pack v1 (Draft)

Ten documents: trust one-pager, DPA template, subprocessors, retention, AI processing, audit handling, security, incidents, residency, buyer privacy

Status: Draft for review. Written to be split into standalone documents once approved. **Legal review required:** the DPA template and any clause with legal effect must be reviewed by qualified counsel before first use. This pack is a working draft, not legal advice. **Two architectural decisions required (flagged in §4):** the erasure-versus-immutable-ledger design, and the source-body retention default. **Placeholders:** items in [square brackets] await internal confirmation of a fact or choice. **Date:** 9 July 2026 · Version 1.0-draft

---

1. Trust & Security One-Pager

(The document a RevOps lead or DPO reads first. One page when formatted.)

PROOF: deliberate capture, human confirmation, attributable evidence — not passive surveillance or autonomous AI decisioning

What PROOF is. PROOF is an evidence governance platform for revenue teams. It holds every claim on a deal to the evidence behind it, separating what a rep asserts from what a buyer has confirmed. Your organisation is the data controller; PROOF is your processor.

What data PROOF processes. Business communications your team chooses to forward (emails, calendar invites), CRM records you connect, and the evidence records derived from them. This includes personal data of your staff and of buyer-side contacts: names, business contact details, and statements attributable to individuals.

The five design facts that matter most:

1. **Humans choose what enters.** PROOF has no passive access to mailboxes or calendars. There is no mailbox OAuth, no background listening, no call recording. Evidence enters by a deliberate human gesture: a forwarded email, a forwarded invite. If your team does not forward it, PROOF never sees it. This is the founding-phase product as shipped; any future mailbox or calendar connection would be opt-in, controller-authorised, scoped, and separately documented before use.
2. **AI proposes; it never writes the record.** AI drafts and summarises. Only a human action (a rep's confirmation) or a buyer's own reply creates a record. No AI output becomes truth on its own, and no AI system can score, judge or pronounce on a deal. This is enforced in the database permission layer, not by policy.

3. **Every piece of personal data is attributed and findable.** PROOF's core function is attribution: every claim is indexed to who said it, when, and on what evidence. A subject access request that takes weeks across a call-recording archive is a query in PROOF. Provenance is our product: it supports your accountability, subject-rights response and auditability by making attributed evidence findable by person, deal, date and source.
4. **Where the Deal Room is enabled, buyer-side individuals can see and challenge what is recorded about them.** Through the Deal Room, your buyers can view the claims attributed to them, and buyer-confirmed evidence only exists where the buyer explicitly confirmed it. Silence is never treated as confirmation. Most sales tools record people without their knowledge; PROOF records claims people confirmed, and shows them the record.
5. **Data stays in Europe.** Production data is hosted in AWS eu-west-1 (Ireland). See the Data Residency Position (§9) for the treatment of AI subprocessing.

Where we are as a company. PROOF is an early-stage company. We do not yet hold SOC 2 or ISO 27001 certification [roadmap: SOC 2 Type I targeted at (date TBD)]. We compensate with architecture: the security properties above are structural (database-enforced permissions, no standing data access, deterministic processing paths) rather than procedural promises. Every claim in this pack is inspectable on request.

The paperwork. A signed DPA (Article 28 compliant) is standard with every subscription. Our subprocessor list, retention policy, and incident position are published and versioned. Contact: [privacy@proofhq.io].

---

2. Data Processing Addendum (Template)

(Skeleton for counsel review. UK GDPR and EU GDPR. Governing law: England and Wales.)

DATA PROCESSING ADDENDUM — between **[Client]** ("Controller") and **[PROOF legal entity name]** ("Processor"), forming part of the Agreement dated [date].

1. Definitions. "Data Protection Laws" means UK GDPR, the Data Protection Act 2018, and where applicable EU GDPR. "Personal Data", "processing", "data subject", "personal data breach" have the meanings in those laws.

2. Scope and roles. Controller determines the purposes and means of processing. Processor processes Personal Data only to provide the PROOF service. Details of processing are at Annex 1.

3. Processor obligations. Processor shall: (a) process Personal Data only on the Controller's documented instructions, including with regard to international transfers, unless required by law (in which case Processor informs Controller unless prohibited); (b) ensure persons authorised to process are bound by confidentiality; (c) implement appropriate technical and organisational measures per Article 32 (summarised at Annex 2, the Security Architecture Summary); (d) respect the subprocessor conditions in clause 5; (e) taking into account the nature of processing, assist Controller by appropriate technical and organisational measures in responding to data subject rights requests (access, rectification, erasure, restriction, portability,

objection); (f) assist Controller with Articles 32 to 36 obligations (security, breach notification, DPIAs) taking into account the information available to Processor; (g) at Controller's choice, delete or return all Personal Data at the end of the service, and delete existing copies unless law requires storage (per the Retention and Deletion Policy, incorporated at Annex 3); (h) make available information necessary to demonstrate compliance, and allow for and contribute to audits conducted by Controller or its mandated auditor, on reasonable notice, no more than [once] per 12 months absent a personal data breach.

4. Data subject rights mechanics. Because PROOF attributes all evidence to identified individuals, Processor can produce, per data subject: all records attributed to them, provenance, and dates. Access and rectification are supported natively, and Processor assists with verified data-subject-rights requests within [5] business days, or faster where reasonably required to meet the Controller's statutory deadlines. Erasure is executed per the anonymisation procedure at Annex 3 [DECISION REQUIRED: see §4 of the Trust Pack — erasure design], which removes the identifiability of the individual while preserving the integrity of the Controller's evidence ledger.

5. Subprocessors. Controller grants general written authorisation to the subprocessors listed at [URL of Subprocessor List]. Processor gives [30] days' notice of intended additions or replacements, during which Controller may object on reasonable data-protection grounds. Processor imposes equivalent obligations on subprocessors and remains liable for their performance.

6. International transfers. Personal Data is hosted in the EEA (AWS eu-west-1). Where a subprocessor processes Personal Data outside the UK/EEA (see Subprocessor List for the AI provider position), transfers are made under [the UK IDTA / EU SCCs Module 3, plus supplementary measures described in the AI/LLM Processing Note], or an adequacy decision where applicable.

7. Personal data breach. Processor notifies Controller without undue delay after becoming aware of a personal data breach affecting Controller's Personal Data, and in any event within [48] hours of confirming that Controller Personal Data is affected, providing the information reasonably required for Controller's own Article 33 obligations. Details: Incident Notification Position (§8), incorporated by reference.

8. Special category data. The PROOF service is not designed or intended to process special category data. Controller instructs its users accordingly. Incidentally captured special category data is handled per §5 of the Retention and Deletion Policy.

9. Term, liability, order of precedence. [Standard clauses: co-terminous with the Agreement; liability per the Agreement; this DPA prevails over the Agreement in respect of Personal Data.]

Annex 1 — Details of processing. - *Subject matter:* provision of the PROOF evidence governance service. - *Duration:* the subscription term plus the deletion window in Annex 3. - *Nature and purpose:* ingestion of Controller-forwarded business communications and connected CRM records; extraction and human-confirmed attribution of deal evidence; rendering of briefs, reviews and governed outputs; publication of confirmed records to Controller's CRM. - *Categories of data subjects:* Controller's personnel (sales and revenue staff);

business contacts of Controller's prospects and customers ("buyer-side contacts"). - *Categories of personal data:* names, business email addresses, job titles, business phone numbers, meeting attendance, and the content of business communications the Controller's users forward, including statements attributable to individuals. No special category data by design (clause 8).

Annex 2: Security Architecture Summary (§7 of this pack). **Annex 3:** Data Retention and Deletion Policy (§4). **Annex 4:** Subprocessor List (§3).

---

3. Subprocessor List

(Published and versioned. [Confirm each row before publication.])

Subprocessor	Purpose	Data touched	Location / region	Transfer mechanism
Supabase (on AWS)	Database, authentication, storage	All service data	**eu-west-1 (Ireland)**	None required (EEA)
Vercel	Application hosting, edge delivery	Data in transit through the application layer	[Confirm: EU region config / global edge]	[SCCs/IDTA if applicable]
[Anthropic]	AI drafting and narration (see AI/LLM Processing Note)	Content of items being drafted/narrated, transiently	[Confirm endpoint region; US if standard API]	[SCCs/IDTA + no-training and zero-retention commitments; see §5]
[Transactional email provider, e.g. Resend/Postmark]	System notifications	Names, email addresses	[Confirm]	[Confirm]
[Error monitoring, e.g. Sentry]	Reliability	Technical logs (metadata only; render logs contain no content bodies)	[Confirm]	[Confirm]

Not subprocessors: the Controller's own Slack workspace, Microsoft Teams tenant, CRM (Salesforce/HubSpot), and email system. PROOF delivers into, and receives from, systems the Controller already operates under its own agreements; PROOF does not appoint them.

---

4. Data Retention and Deletion Policy

1. **During the subscription:** evidence records, attribution and audit trails are retained for the life of the subscription. That persistence is the product: the ledger is the Controller's governed record. 1a. **Source communications (the forwarded item itself).** Retention is purpose-bound: source bodies are retained **only for items that became evidence** — so every citation terminates in a real, producible artefact under audit challenge — and forwarded items that never minted a record are deleted after [30] days. A cryptographic hash of every processed source is always retained (proving what was seen without keeping it). A stricter client-configurable mode is available: extract-plus-metadata-plus-hash only, no source bodies, where the Controller prefers maximum minimisation and accepts the reduced evidential weight. **[DECISION REQUIRED: ratify this default; it interacts with the erasure design in item 4 and needs the same schema session.]**
2. **On termination:** full export available in machine-readable form for [30] days. All Controller data deleted within [60] days of termination, confirmed in writing. Backups age out within a further [30] days.
3. **Render and operational logs:** contain metadata only (timestamps, deal identifiers, trigger types), never the content of briefs or evidence. Retained [12] months for reliability and fair-usage measurement, then deleted.
4. **Individual erasure requests (the ledger question).** PROOF's ledger is immutable by design: evidence is superseded, never silently edited, because that is what makes it defensible. Erasure rights are honoured by **anonymisation rather than row deletion**: on a verified erasure instruction from the Controller, the individual's identifiers (name, email, phone, free-text identifying references) are removed or replaced with a non-identifying marker across the evidence chain, and the identity record is destroyed. The chain's structure and dates persist; the person is no longer identifiable from it. **[DECISION REQUIRED — recommended design:** hold personal identifiers in a separable identity layer referenced by the evidence chain, so erasure is the destruction of the identity record plus scrubbing of free-text references, executed as one auditable operation. This preserves ledger integrity and makes erasure provable. Requires a schema decision before first placement.**]**
5. **Incidentally captured sensitive data:** PROOF does not intentionally process special category data, and extraction never creates claims from it. Where a forwarded item incidentally contains such data (for example a passing reference to illness), it is not indexed as evidence, and the source item is deleted on Controller request.
6. **Audit engagements:** see §6. Nothing is retained.

---

5. AI / LLM Processing Note

What AI does in PROOF: drafts (evidence records, follow-up emails, briefs) and narrates (cited answers over the record). **What AI cannot do:** create a record, confirm evidence, score a deal, or write to the system of truth. Three acts create records in PROOF: a rep's confirmation

tap, a rep's decision to send, a buyer's explicit reply. All three are human. This separation is enforced at the database permission layer and continuously verified by automated checks.

Grounding and citation: AI narration is constrained to retrieved records; every factual sentence must cite the underlying record or it is removed before display. Numbers are never computed by the model.

Provider commitments [confirm against provider terms before publication]: client data submitted to the AI provider is **not used to train models**; API processing is transient with [zero data retention configured / retention limited to (X) days for abuse monitoring]; provider is bound as a subprocessor with equivalent obligations. Endpoint region: [confirm; if US, transfers proceed under SCCs/IDTA with the supplementary measures of transience, no-training, and content minimisation].

Content minimisation: the model receives the item being drafted or the records being narrated, not the corpus. There is no bulk export of the Controller's ledger to any AI system.

No automated decision-making: PROOF does not conduct solely automated decision-making producing legal or similarly significant effects on individuals (UK/EU GDPR Article 22). Every record-creating and commercially consequential act in PROOF is human.

Fair usage: AI usage is included in the subscription under a published fair-usage line; usage is metered by PROOF internally for cost integrity, never billed per use.

---

6. Audit Data Handling Note (Evidence Audit engagements)

The Evidence Audit is a one-time diagnostic performed on a CRM export you provide. Its data handling is deliberately stricter than the subscription service:

1. **No persistence.** The audit pipeline stores nothing: your export is processed, the findings document is generated, and the working data is destroyed on completion of the run. There is no audit database for your data to sit in.
2. **Point-in-time, export-based.** No standing connection to your systems, no API credentials, no OAuth. You produce an export; you can inspect exactly what you handed over.
3. **What is retained:** the findings document (yours), and an engagement record containing only: your organisation's name, the sponsoring signatory, the consent reference, a cryptographic hash of the dataset (proving what was analysed without retaining it), the rules version, and the run date.
4. **Findings are pipeline-level.** The client-facing deliverable contains no individual-level findings about your staff.
5. **Verification:** the no-residue property is tested as part of the audit software's release process (a post-run filesystem check), and the methodology behind every finding is published in the deliverable's appendix.

---

7. Security Architecture Summary

(Honest for an early-stage company: structural controls stated as facts, organisational maturity stated as roadmap.)

Access control at the database, not the application. Every table is protected by row-level security in PostgreSQL. Client organisations are isolated at the database layer; partner access is isolated the same way and adversarially tested (a hostile principal from another organisation or partner receives zero rows, denied by the database, not hidden by the interface).

Least privilege for machines. AI and agent components hold database roles with **no write permissions** to the system of record — grants are absent at the PostgreSQL level, and an automated integrity check fails the build if any such grant appears. The single computation that produces governance rollups has exactly one writer.

Encryption. TLS 1.2+ in transit; AES-256 at rest (managed by Supabase/AWS). Secrets held in managed environment stores, never in code.

Data minimisation by architecture. No passive ingress (nothing enters without a human gesture); operational logs carry metadata, never content; the audit pipeline persists nothing; buyer-facing surfaces expose only what the querying principal is entitled to see, enforced by the same row-level security.

Change control. All schema changes are versioned migrations; production changes pass automated integrity checks (including the machine-write-permission check above) before deployment; verification against the live rendered output is a release requirement.

Environment separation. Production, demo and test organisations are distinct; demo environments contain synthetic data only.

Organisational measures (current, stated honestly): [single-founder operation with (contractor?) access as applicable]; access to production limited to [named roles/individuals]; MFA on all administrative accounts; [SSO for client users: roadmap/available]. **Certifications:** none yet; SOC 2 Type I is on the roadmap [target date]; this summary and the DPA are offered in the interim, with architecture inspectable on request.

Annex form — Technical and Organisational Measures (TOMs), for DPA Annex 2: Access control (RLS at the database; org and partner isolation adversarially tested) · MFA on all administrative accounts · Encryption (TLS 1.2+ transit, AES-256 rest) · Tenant isolation (Postgres-enforced) · Least-privilege machine roles (no AI/agent write grants, build-failing integrity check) · Logging and monitoring (metadata-only operational logs; error monitoring) · Backup and recovery (§11) · Vulnerability management (dependency scanning; disclosure route §8.6; independent test on roadmap) · Change control (versioned migrations; automated integrity gates; render-verified releases) · Personnel confidentiality (written obligations for all with production access) · Subprocessor due diligence (equivalence obligations, §3 list, notice per DPA clause 5) · Secure deletion (§4, including no-persistence audit pipeline and anonymisation-based erasure).

---

8. Incident Notification Position

1. **Definition:** a personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
2. **Notification to you (the Controller):** without undue delay after we become aware, and in any event within **[48] hours of confirming that your personal data is affected**, by email to your nominated contact, with: nature of the breach, categories and approximate numbers of data subjects and records, likely consequences, measures taken or proposed, and a named contact.
3. **Rolling updates:** as material facts emerge, so your own 72-hour regulator obligations are never gated on us.
4. **We do not notify regulators or data subjects on your behalf** (that is the Controller's decision and duty); we provide everything reasonably needed for you to do so.
5. **Post-incident:** a written root-cause summary within [10] business days of resolution, including corrective measures.
6. **Security contact:** [security@proofhq.io]. Suspected vulnerabilities are acknowledged within [2] business days; good-faith reporting is welcomed [and will not be subject to legal action — safe harbour statement to confirm with counsel].

---

9. Data Residency Position

1. **System of record:** all evidence, attribution, and audit-trail data is stored in **AWS eu-west-1 (Ireland)** via Supabase. Backups remain in-region.
2. **Application layer:** hosted on Vercel [confirm region configuration; state plainly whether edge nodes outside the EEA transit data].
3. **AI processing:** the only routine flow of content outside the EEA [if applicable per provider endpoint] is transient AI drafting/narration, under the transfer mechanism and commitments in the AI/LLM Processing Note: no training, no retention beyond [X], content minimisation. [If an EU endpoint is available from the provider, state: AI processing is EU-resident, and this section reduces to one line.]
4. **Client-side systems:** data PROOF publishes to your CRM or delivers into your Teams/Slack resides wherever your tenancy resides, under your agreements.
5. **UK clients:** the UK–EU adequacy arrangements apply to EEA hosting; the DPA addresses both UK GDPR and EU GDPR.

---

10. Buyer-Data and Deal Room Privacy Explanation

(Written to be shown to a client's buyer if ever asked: "what does this tool hold about me?")

What PROOF records about buyer-side people. When a seller forwards a business communication you were part of, PROOF may record: your name and business contact details,

your attendance at meetings, and claims attributed to you (for example, “confirmed budget approval on 12 June”), each linked to its source.

What makes PROOF different from recording tools: - **Nothing is captured passively.** PROOF does not record calls, read mailboxes, or monitor anyone. It only ever processes items a human deliberately forwarded. - **“Buyer-confirmed” means you confirmed it.** The highest grade of evidence in PROOF exists only where you explicitly replied confirming a point. Your silence is never treated as agreement; an unanswered email confirms nothing. - **You can see the record.** Through the Deal Room, you can view what has been attributed to you on a deal, and challenge it: a disputed point is marked contested, not quietly kept. - **AI never characterises you.** No AI system in PROOF scores you, profiles you, infers your sentiment, or writes judgements about you into any record. AI drafts text for humans to review; only humans and you create records. - **Your rights** (access, correction, erasure) are exercised through the selling organisation (the data controller); PROOF supports them natively, including erasure by anonymisation that removes your identifiability from the record.

In one sentence: most sales tools record people without their knowledge; PROOF records claims people confirmed, and shows them the record.

---

11. Business Continuity and Backup Position

1. **Backups:** the system of record is backed up daily, with point-in-time recovery enabled [confirm PITR window, e.g. 7/14 days] via Supabase/AWS. Backups remain in-region (eu-west-1) and age out per the Retention Policy.
2. **Recovery targets (stated honestly for our stage):** recovery point objective [24 hours or better with PITR]; recovery time objective [target: same business day]. These are engineering targets, not contractual SLAs, and are reviewed as the client base grows.
3. **Restore verification:** backup restoration is tested [quarterly — confirm cadence] against a non-production environment; the most recent test date is available on request.
4. **Dependencies:** continuity of the application layer (Vercel) and database layer (Supabase/AWS) inherits those providers’ own resilience commitments; PROOF’s architecture holds no client data outside those managed platforms.
5. **Client-side resilience:** governed state published to your CRM remains in your CRM regardless of PROOF availability — the Publisher means your system of record is never solely dependent on ours.

---

12. Support Access and Personnel Position

(The solo-operation question, answered before it is asked.)

1. **Who can access production:** a named, minimal set of individuals [currently: the founder, plus [named contractor roles] as applicable]. There is no support team with standing data access, because there is no data access we have not listed.

2. **Support access to client content** happens only where required to provide support, investigate an incident, maintain the service, or comply with law — with the client's permission for support matters, limited to authorised personnel, logged, time-bound where possible, and restricted to the minimum data necessary. Routine support is performed against metadata and synthetic environments first.
3. **Administrative access controls:** MFA on all administrative accounts; production credentials held in managed secret stores; no shared accounts.
4. **Personnel:** all persons with any production access are bound by written confidentiality obligations. [Background checks: state position.]
5. **Engineering access model:** automated agents and AI components hold database roles with no write access to client truth (see §7); human production access is the exception, not the operating model.

---

13. AI Regulation Position (EU AI Act and equivalents)

1. **Risk classification:** PROOF assesses its AI features as **limited/minimal risk** under the EU AI Act. The high-risk category most plausibly adjacent to sales tooling is AI used for **monitoring and evaluating workers**. PROOF is architecturally outside it, by documented refusal: no rep scoring, no behavioural profiling, no productivity surveillance surfaces, no AI evaluation of any individual's performance, and no outcome predictions about people. These are permanent product refusals, not configuration defaults.
2. **Transparency obligations:** AI-drafted content is always presented to a human for review before any record or communication exists; users interact with AI features knowingly; AI narration is citation-bound to retrieved records.
3. **Human oversight by design:** the three record-creating acts in PROOF (rep confirmation, rep send, buyer confirmation) are human. This is the Act's human-oversight principle implemented at the database permission layer.
4. **No emotion recognition, no biometrics, no social scoring** — none of the prohibited-practice categories are present in any form.
5. **Review cadence:** this position is reviewed against final implementing guidance [and at each pricing/product revision gate].

---

14. Insurance and Availability Position

1. **Cyber liability insurance:** [confirm status — held with (insurer), £(limit) / in procurement, target (date)]. Certificate available on request once in force.
2. **Availability posture:** target availability [99.5%+] measured monthly; planned maintenance announced in advance; material incidents communicated to nominated contacts per §8. This is a stated posture for the founding phase, not a contractual SLA; SLA terms are available for Assurance-tier clients on request [decide].

3. **Status communication:** [status page / email to nominated contacts — confirm mechanism].

---

15. DPIA Support Statement

Where the Controller determines that a Data Protection Impact Assessment is required — for example, for processing buyer communications through an LLM in a larger or regulated organisation — PROOF provides reasonable assistance: this Trust Pack, data-flow descriptions, the subprocessor list and transfer mechanisms, retention and deletion positions, the TOMs annex, and answers to reasonable follow-up questions, within [5] business days of request.

---

16. Trust Change Notice

This pack is versioned. Material changes — subprocessor additions or replacements, retention changes, residency changes, material security-measure changes — are notified to nominated client contacts with [30] days' notice (per DPA clause 5 for subprocessors), with a published change log [on the proofhq.io trust page]. Clients may object to subprocessor changes on reasonable data-protection grounds within the notice window.