

CONTRACTUAL TEMPLATE

PROOF Data Processing Addendum Template

A customer-specific processor agreement template for completion and qualified legal review.

TEMPLATE - COUNSEL REVIEW REQUIRED

Version 1.1 | 20 September 2026 | proofhq.io/trust

The current signed agreement controls where it differs from this document.

Data Processing Addendum for customer-specific review.

This template is a drafting aid for qualified counsel. It is not an executed agreement and must be completed, reviewed and signed for the relevant customer and deployment.

Counsel review required

Complete every bracketed field, attach the applicable transfer terms and confirm the operational schedules before signature. The signed version controls over this template.

Field	To be completed
Controller	[CUSTOMER LEGAL NAME AND ADDRESS]
Processor	[PROOF LEGAL ENTITY NAME AND ADDRESS]
Agreement	[MASTER AGREEMENT AND EFFECTIVE DATE]
Governing law	[AS AGREED IN THE MASTER AGREEMENT]
Privacy contacts	Customer: [EMAIL] PROOF: privacy@proofhq.io

Core processing terms.

This Data Processing Addendum forms part of the agreement identified on the cover page between the Controller and Processor.

1. Definitions

- 1.1 Applicable Data Protection Law means the UK GDPR, the Data Protection Act 2018, the EU GDPR where applicable, and other laws identified in the Agreement.
- 1.2 Controller, Processor, Personal Data, Processing, Data Subject, Supervisory Authority and Personal Data Breach have the meanings given by Applicable Data Protection Law.
- 1.3 Customer Data means Personal Data processed by Processor on behalf of Controller in providing the PROOF service.
- 1.4 Sub-processor means a third party appointed by Processor to process Customer Data on behalf of Controller.

2. Scope and roles

- 2.1 Controller determines the purposes and means of Processing. Processor processes Customer Data only to provide the services and on Controller's documented instructions, including the Agreement, this Addendum and authorised use of the service.
- 2.2 The subject matter, duration, nature, purpose, Data Subjects and categories of Personal Data are described in Annex 1.
- 2.3 Controller is responsible for the lawfulness and accuracy of its instructions and for providing required notices or obtaining required permissions.

Confidentiality, security and assistance.

Processor applies the obligations below to Customer Data processed under the Agreement.

3. Processing instructions and confidentiality

- 3.1 Processor will process Customer Data only on documented instructions unless required by applicable law. Where legally permitted, Processor will inform Controller before that required processing.
- 3.2 Processor will ensure that people authorised to process Customer Data are bound by confidentiality obligations and receive access only where necessary for their role.
- 3.3 Processor will inform Controller if, in its reasonable opinion, an instruction infringes Applicable Data Protection Law and may suspend that instruction while the parties resolve it.

4. Security

- 4.1 Processor will implement and maintain appropriate technical and organisational measures taking account of the nature, scope, context and purposes of processing and the risk to Data Subjects.
- 4.2 The current measures are described in the PROOF Technical and Organisational Measures document incorporated into this Addendum as Annex 2.
- 4.3 Processor may update the measures where the overall protection is not materially reduced and will communicate material changes through the applicable change process.

5. Data Subject requests

- 5.1 Taking account of the nature of Processing, Processor will provide reasonable technical and organisational assistance to Controller in responding to verified requests to exercise Data Subject rights.
- 5.2 If Processor receives a request directly, it will refer the requester to Controller unless law requires a different response.

The production data path remains controlled.

Customer-specific schedules must reflect the active production deployment at signature.

6. Sub-processors

- 6.1 Controller grants general written authorisation for the Sub-processors listed in Annex 3.
- 6.2 Processor will impose data-protection obligations on each Sub-processor that provide materially equivalent protection for Customer Data and remains responsible for its Sub-processors as required by law.
- 6.3 Processor will give 30 days' notice of intended material additions or replacements. Controller may object on reasonable data-protection grounds during that period. The parties will work in good faith to resolve the objection.

7. International transfers

- 7.1 Processor will not transfer Customer Data outside the UK or EEA unless a lawful transfer mechanism applies.
- 7.2 Where required, the parties will incorporate the applicable EU Standard Contractual Clauses, UK Addendum or International Data Transfer Agreement identified in the Order Form or transfer schedule.
- 7.3 The customer-specific Sub-processor and Data Residency Statement records the active locations and transfer position for the deployment.

8. Personal Data Breaches

- 8.1 Processor will notify Controller without undue delay after becoming aware of a Personal Data Breach affecting Customer Data.
- 8.2 Processor will provide information reasonably available about the nature of the breach, affected Data Subjects and records, likely consequences, containment, recovery and contact point, with rolling updates as material facts become available.
- 8.3 Processor's notice does not constitute an admission of fault or liability.

Evidence of compliance remains proportionate and secure.

The parties should align these clauses with the liability, confidentiality and audit provisions in the main Agreement.

9. Assistance and audit information

- 9.1 Taking account of the nature of Processing and information available, Processor will provide reasonable assistance with security, breach notification, impact assessments and prior consultation obligations.
- 9.2 Processor will make available information reasonably necessary to demonstrate compliance with this Addendum, including current trust documents and completed security questionnaires.
- 9.3 If that information is insufficient, Controller may request an audit by an independent auditor bound by confidentiality, on reasonable notice, during normal business hours and no more than once in any 12-month period unless required by law or following a material breach.

10. Return and deletion

- 10.1 At the end of the services, Processor will, at Controller's choice and subject to the Agreement, return or delete Customer Data and delete existing copies unless applicable law requires retention.
- 10.2 Export windows, primary deletion and backup expiry follow the customer-specific retention schedule.
- 10.3 Verified individual erasure instructions are executed using the applicable de-identification or deletion process while preserving only non-identifying structure required for the governed record.

11. Order of precedence and term

- 11.1 This Addendum begins on the effective date of the Agreement and continues while Processor processes Customer Data.
- 11.2 If there is a conflict about Personal Data, this Addendum prevails over the Agreement unless the signed documents expressly state otherwise. Applicable transfer terms prevail where required by law.
- 11.3 Liability, governing law and dispute resolution follow the Agreement unless mandatory law requires otherwise.

Details of processing.

Complete and verify this schedule for the customer deployment before signature.

Item	Description
Subject matter	Provision of the PROOF revenue decision platform and agreed implementation, support and assurance services.
Duration	The subscription term plus the export, deletion and backup-expiry periods in the agreed retention schedule.
Nature and purpose	Ingest authorised CRM records and structured evidence; retain attribution and decision history; prepare evidence-bound outputs; support authorised publication to customer systems.
Data Subjects	Customer personnel and business contacts of customer prospects or customers, including buyer-side contacts.
Personal Data	Names, business contact details, job information, meeting attendance, CRM identifiers and business statements or communications deliberately supplied through authorised routes.
Special category data	Not intentionally required or designed for the service. Controller instructs users not to submit it unless expressly agreed.
Frequency	Continuous during authorised service use.
Controller instructions	The Agreement, this Addendum, authorised configuration and documented customer instructions.

Security measures and Sub-processors.

Attach the current documents identified below to the executed Addendum.

Annex 2 PROOF Technical and Organisational Measures, version and date recorded at signature.	Annex 3 PROOF Sub-processors and Data Residency Statement, version and date recorded at signature.
Supporting policy PROOF Retention Deletion and Data Rights Statement.	Supporting position PROOF Incident Response and Business Continuity Statement.

Execution

Do not sign this generic template. Counsel must confirm the legal entities, governing agreement, transfer mechanism, customer-specific schedules and signature blocks.

Signatures

For Controller	For Processor
Name: [NAME] Title: [TITLE] Signature: [SIGNATURE] Date: [DATE]	Name: [NAME] Title: [TITLE] Signature: [SIGNATURE] Date: [DATE]