

THREATVIEW

Merchant Data Processing Addendum

GDPR processor terms for the ThreatView service with technical and organisational measures

Document information	Details
Processor	Turaco Labs Limited
Company	Company number 15368842; incorporated in England and Wales
Parent company non-party	Turaco Labs, company number C204814 GBC, registered at AMG Services Ltd, 11th Floor, Tower A, 1 Exchange Square, Ebene, Mauritius. Turaco Labs is the holding company of Turaco Labs Limited and is not a party to this Addendum.
Registered office	2 Old Bath Road, Newbury, Berkshire, RG14 1QL, United Kingdom
Merchant	The customer identified in the applicable Agreement or Order
Effective date	6 October 2026; for each Merchant, contractually effective when incorporated into an Agreement or Order or accepted through the separate authenticated electronic route
Version and status	1.4 - effective 6 October 2026; revised 9 October 2026
Reference date	9 October 2026
Privacy contact	Niall Newman, Privacy Officer - nn@turacolabs.com
Authorised Turaco signatory	Benjamin Hosack, Chief Executive Officer

Scope of this Addendum

This Addendum sets out how Turaco Labs Limited processes Merchant Personal Data for core ThreatView services and the technical and organisational measures protecting it. It applies when incorporated into the applicable Agreement or Order. External partner PCI integration plans are available only to organisations in Australia and New Zealand, and European customer organisations have no access to that integration. Processing under those plans requires separate programme-specific disclosures, terms and authorisation.

Contents

- 1 Parties and status
- 2 Definitions and interpretation
- 3 Scope precedence and processing details
- 4 Documented instructions
- 5 Confidentiality and personnel
- 6 Security of processing
- 7 Subprocessors
- 8 International transfers
- 9 Data subject rights
- 10 Security incidents and personal data breaches
- 11 Data protection impact assessment and consultation
- 12 Information audit and assurance
- 13 Return, deletion and end of services
- 14 Government and third-party requests
- 15 Liability term and general provisions
- Schedule 1 Processing particulars
- Schedule 2 Technical and organisational measures
- Schedule 3 Supplier, subprocessor and transfer governance
- Schedule 4 Execution

Defined terms carry the meanings in Section 2 and the Agreement.

1 Parties and status

This Data Processing Addendum is entered into between the customer identified in the Agreement or applicable Order (the "Merchant") and Turaco Labs Limited, company number 15368842, whose registered office is 2 Old Bath Road, Newbury, Berkshire, RG14 1QL, United Kingdom ("Turaco"). Turaco Labs Limited is a subsidiary of Turaco Labs, company number C204814 GBC, registered at AMG Services Ltd, 11th Floor, Tower A, 1 Exchange Square, Ebene, Mauritius (the "Mauritius Parent"). The Mauritius Parent is a holding company and a separate legal entity. It is not a party to this Addendum and does not receive Merchant Personal Data through Turaco's personnel arrangements. Turaco Labs Limited remains the contracting entity and the Processor responsible to the Merchant for performance of this Addendum.

For Personal Data contained in Merchant Data and processed by Turaco to provide ThreatView, the Merchant acts as Controller and Turaco acts as Processor, except where applicable law assigns a different role. Turaco acts as an independent Controller for its own Account Data, workforce, supplier, billing, business correspondence and contractual records, optional marketing and sales-management, legal-compliance and service-security records as described in the ThreatView Privacy Notice.

Where the Merchant is itself a Processor for another Controller, Turaco acts as the Merchant's Subprocessor. The Merchant represents that it is authorised to appoint Turaco and issue the documented instructions recorded in the Agreement. To the extent required for Turaco's Article 30(2) records, the Merchant shall provide the relevant Controller's name and contact details and any applicable representative or Data Protection Officer details. Turaco may maintain those details in its existing customer or contract records.

This Addendum provides the processor terms required by Article 28 UK GDPR and, where EU GDPR applies to the relevant processing, Article 28 EU GDPR.

2 Definitions and interpretation

Term	Meaning
Agreement	The Order, service terms, licence terms or other written agreement under which Turaco provides ThreatView to the Merchant. Commercial liability provisions apply to this Addendum only when expressly incorporated into and accepted under that Agreement.
Applicable Data Protection Law	The UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and any other binding privacy or data-protection law applicable to the processing. EU GDPR is included where it applies.
Controller, Processor, Data Subject, Personal Data, Processing and Supervisory Authority	Have the meanings given by Applicable Data Protection Law.
Merchant Data	Data supplied by or for the Merchant, obtained from Merchant-authorized systems, or generated for the Merchant through ThreatView, including Merchant Security Data.
Merchant Security Data	Security, assessment, monitoring, event, finding, incident, evidence, configuration and related data processed to provide ThreatView.
Personal Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.
Restricted Transfer	A transfer of Personal Data that requires a safeguard or other transfer mechanism under Applicable Data Protection Law.
Subprocessor	A third party engaged by Turaco to process Merchant Personal Data on behalf of the Merchant, excluding Turaco Personnel.
Mauritius Parent	Turaco Labs, company number C204814 GBC, registered at AMG Services Ltd, 11th Floor, Tower A, 1 Exchange Square, Ebene, Mauritius, being the holding company of Turaco Labs Limited.
Turaco Personnel	Turaco employees and directly engaged individuals who process Merchant Personal Data solely under Turaco's direct authority and documented instructions, including persons serving in roles comparable to employees for data-protection purposes.

References to writing include authenticated electronic instructions. A requirement not to do something includes a requirement not to permit it. If the UK GDPR and EU GDPR both apply, each obligation is read to meet the stricter applicable requirement without duplicating performance.

3 Scope precedence and processing details

This Addendum applies to Turaco's processing of Merchant Personal Data as Processor in connection with the core ThreatView service. The separately offered Australia/New Zealand-only partner PCI integration is outside the scope of this core-service edition and requires its own relevant processing terms and authorisation. Schedule 1 specifies the subject matter, duration, nature, purpose, Personal Data types and Data Subject categories.

If this Addendum conflicts with another part of the Agreement about processing Merchant Personal Data, this Addendum prevails to the extent of that conflict. A signed transfer addendum or mandatory statutory term prevails for the Restricted Transfer it governs. Liability provisions in the Agreement apply to this Addendum only to the extent expressly incorporated and permitted by law, subject to Section 15.

The Merchant Data Processing Policy provides service transparency and is not a substitute for this Addendum. The Supplier, Subprocessor and International Transfer Register is an operational record; a provider qualifies as a Subprocessor according to law and actual processing, not merely by the label assigned in a register.

4 Documented instructions

Turaco shall process Merchant Personal Data only on the Merchant's documented instructions, including instructions concerning Restricted Transfers, unless required to process by UK, retained EU or other law binding on Turaco. In that event Turaco shall inform the Merchant of the legal requirement before processing unless the law prohibits that notice for an important public-interest reason.

The Agreement, configured service scope, authorised-user actions, documented support requests and this Addendum constitute the Merchant's initial instructions. Turaco shall not sell Merchant Personal Data, disclose it to data brokers, use it for third-party advertising, use it for unrelated model training, or use it to build an unrelated commercial profile.

Turaco shall promptly inform the Merchant if, in Turaco's reasonable opinion, an instruction infringes Applicable Data Protection Law. Turaco may suspend the affected processing while the parties resolve the issue and shall continue unaffected processing where reasonably possible.

The Merchant is responsible for the lawfulness, fairness and accuracy of its instructions; its authority over monitored systems and data; notices and lawful bases owed to Data Subjects; and minimising special-category, criminal-offence, authentication-secret and unrelated personal data supplied to ThreatView.

5 Confidentiality and personnel

- Turaco shall ensure that persons authorised to process Merchant Personal Data are bound by contractual or statutory confidentiality obligations and receive access only for an authorised role.
- Access shall follow least-privilege and need-to-know principles, use individual or attributable service identities, and be removed or changed when duties change or access is no longer required.
- Personnel with administrative or support access shall receive appropriate privacy and security instruction and be subject to disciplinary and incident-management processes.
- Turaco shall preserve an auditable record of security-relevant administrative, credential and remote-access operations in accordance with the technical measures in Schedule 2.

6 Security of processing

Taking account of the state of the art, implementation cost, the nature, scope, context and purposes of processing, and the risk to individuals, Turaco shall implement and maintain appropriate technical and organisational measures designed to protect Merchant Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

The standard measures are set out in Schedule 2. Turaco may update a measure to reflect technical development, provided the update does not materially reduce the overall protection of Merchant Personal Data. Turaco shall document material changes through its controlled security and supplier-governance processes.

Merchant-specific security obligations, if any, must be recorded in the Agreement or Order. Security descriptions are not a warranty that every threat can be prevented, but Turaco shall operate the stated controls with appropriate diligence and test or review their effectiveness in proportion to risk.

7 Subprocessors

The Merchant grants Turaco general written authorisation to appoint Subprocessors needed to provide ThreatView, subject to this Section. Turaco shall publish the current Merchant-facing Subprocessor List at [Turaco Labs Data Processing and GDPR](#) and give at least 30 days' advance notice by email of an intended addition or replacement that will process Merchant Personal Data.

The Merchant may object during the 30-day notice period on reasonable, documented data-protection grounds by emailing support@turacolabs.com. The parties shall work in good faith to resolve the objection, including by applying additional safeguards, avoiding the affected processing where reasonably available, or agreeing an orderly termination of the affected feature. If no reasonable solution is available, the Merchant may close the affected account before the change takes effect.

Before a Subprocessor begins processing, Turaco shall complete proportionate due diligence and impose a written contract that provides data-protection obligations no less protective, in substance, than those applicable to Turaco for the relevant processing. Turaco remains responsible to the Merchant for the Subprocessor's performance to the extent required by Applicable Data Protection Law and the Agreement.

Infrastructure ownership, encryption or lack of routine provider access does not by itself settle whether a supplier is a Subprocessor. Turaco shall classify each service according to the contract, technical access and actual data flow and shall correct the register if those facts change.

A directly engaged individual acting solely as Turaco Personnel is not a Subprocessor merely because the person is a contractor or holds an unrelated office in another group company. The Mauritius Parent does not process or receive Merchant Personal Data and is not a Subprocessor. Turaco shall reassess the role and complete any required Merchant authorisation and Article 28 terms before permitting access for a parent-company purpose, through parent-company systems or on parent-company instructions.

8 International transfers

Turaco shall not make a Restricted Transfer of Merchant Personal Data unless instructed or authorised by the Merchant and supported by a lawful transfer mechanism. Where required, Turaco shall use an applicable UK adequacy regulation, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, applicable EU Standard Contractual Clauses, binding corporate rules or another legally valid mechanism.

Before relying on contractual safeguards, Turaco shall complete and document the required transfer risk assessment or data protection test, consider destination-country law and practical access risk, and implement supplementary technical, contractual or organisational measures where necessary. A certification such as the EU-US Data Privacy Framework shall be relied upon only after current participation and scope are verified.

Turaco's Supplier, Subprocessor and International Transfer Register records destinations, roles, mechanisms and transfer assessments.

9 Data subject rights

Taking account of the nature of the processing, Turaco shall provide reasonable technical and organisational assistance to enable the Merchant to respond to requests to exercise Data Subject rights. This includes available search, export, correction, restriction and deletion capabilities and appropriately scoped operational assistance.

If Turaco receives a request relating to Merchant Personal Data, it shall not respond on the merits unless authorised or legally required. Turaco shall promptly direct the requester to the Merchant where appropriate and notify the Merchant, unless prohibited by law. The Merchant remains responsible for determining the response and applicable exemptions.

10 Security incidents and personal data breaches

Turaco shall notify the Merchant without undue delay after becoming aware of a Personal Data Breach affecting Merchant Personal Data. Notification does not constitute an admission of fault or liability.

To the extent information is available, Turaco shall provide the nature of the breach; categories and approximate numbers of affected Data Subjects and records; likely consequences; measures taken or proposed; relevant dates; and a contact point. Turaco may provide information in phases where doing so avoids delay.

Turaco shall take reasonable steps to contain, investigate, remediate and document the breach; preserve relevant evidence; and assist the Merchant with risk assessment, notification to a Supervisory Authority and communication to Data Subjects where required. Turaco shall not notify a regulator or affected person on the Merchant's behalf without instruction, except where law requires Turaco to do so in its own capacity.

11 Data protection impact assessment and consultation

Taking account of the information available and the nature of processing, Turaco shall provide reasonable assistance with the Merchant's data protection impact assessments and prior consultation obligations under Articles 35 and 36 UK GDPR or equivalent law. Assistance may include processing descriptions, security measures, data flows, supplier details and risk information reasonably necessary for the assessment.

The Merchant remains responsible for deciding whether a DPIA or prior consultation is required for its purposes, monitored environment and Data Subjects.

12 Information audit and assurance

Turaco shall make available information reasonably necessary to demonstrate compliance with this Addendum and Article 28 UK GDPR. It shall allow for and contribute to audits and inspections conducted by the Merchant or an independent auditor mandated by the Merchant, subject to reasonable confidentiality, security, scope and scheduling controls.

The parties shall first use current policies, control descriptions, test results and other remote evidence where these reasonably satisfy the assurance objective. On-site or intrusive testing must not expose another merchant's data, weaken production security, interrupt service, or require disclosure of HSM keys, private keys, exploitable secret material or information Turaco is legally prohibited from disclosing.

Audits shall be proportionate to risk. Additional evidence or audit may be justified after a material breach, a material processing change, a Supervisory Authority request or credible evidence of non-compliance. Each party bears its own costs unless the Agreement or a substantiated material non-compliance requires another allocation.

13 Return, deletion and end of services

At the Merchant's choice and on termination of the relevant services, Turaco shall return or delete Merchant Personal Data and delete existing copies unless binding law requires storage. A request must be authenticated and made by an authorised Merchant representative. Turaco may retain the minimum data necessary to establish legal compliance, resolve a dispute, meet a legal hold or satisfy another binding obligation.

Excluding protected backups and data that law requires Turaco to retain, Turaco shall purge live Merchant Data within 30 days after a valid deletion request. Database and service backups are retained for no longer than 12 months and then expire through the backup lifecycle. Data in a backup is not restored for ordinary use; if a backup is restored, deletion and restriction instructions shall be re-applied before normal processing resumes.

Account closure without a deletion request permits limited Controller-side account records to be kept for reactivation for up to two years after closure. It is not an independent instruction to retain all Merchant Personal Data after service termination. Legal holds are recorded in the database and reviewed at least weekly by system administrators. Deletion resumes automatically when the hold is released. Holds must relate to an applicable obligation or necessary preservation purpose, be limited to relevant records and remain access-restricted.

On request, Turaco shall provide reasonable confirmation of completion and identify any remaining category, legal basis and expected expiry. Turaco may irreversibly anonymise data instead of deleting it only where the result can no longer identify an individual or merchant and no contractual term prohibits that treatment.

14 Government and third-party requests

Unless prohibited by law, Turaco shall notify the Merchant promptly of a legally binding demand for Merchant Personal Data. Turaco shall review the demand for validity, challenge over-broad or unlawful requests where there are reasonable grounds, disclose only the minimum legally required data, and document the request and response.

Nothing in this Addendum requires a party to obstruct lawful process. Turaco shall direct voluntary requests to the Merchant where the Merchant is the appropriate Controller.

Turaco shall maintain the Processor records required by Article 30(2) UK GDPR and, where applicable, Article 30(2) EU GDPR, and cooperate with a competent Supervisory Authority as required by law. Standard processing profiles are linked to existing customer and contract records to identify each Controller, the applicable processing categories and international transfers.

15 Liability term and general provisions

This Addendum begins when it is incorporated into or executed with the Agreement and continues for as long as Turaco processes Merchant Personal Data on the Merchant's behalf. Confidentiality, audit, incident, transfer and deletion obligations survive to the extent necessary to protect retained data and complete required actions.

Limitations of liability, exclusions and indemnities in the Agreement apply to this Addendum only to the extent expressly incorporated and permitted by law. Nothing restricts non-excludable liability, Data Subject remedies, regulator powers or mandatory statutory contribution rights. The governing law and jurisdiction provisions of the Agreement apply, subject to mandatory law.

Contractual notices shall be in writing to the notice address or email recorded in the Order, or a replacement notified in writing. Turaco privacy/security notices may be sent to nn@turacolabs.com; complaints and Subprocessor objections to support@turacolabs.com. The Merchant contact is the Order/account primary contact. Statutory routes and service of proceedings remain governed by applicable law. No notice form restricts a valid Data Subject request.

The parties shall attempt in good faith to resolve a dispute through authorised representatives, without restricting either party's right to seek urgent relief or exercise a statutory remedy. Neither party may assign this Addendum separately from the Agreement.

No change to this Addendum is effective merely because an operational register is updated. Turaco may update security or supplier detail as expressly allowed above; a change to substantive contractual rights requires the mechanism specified in the Agreement.

Schedule 1 Processing particulars

Required detail	Processing description
Subject matter	Provision, operation, support, security and improvement of ThreatView's merchant-authorised security monitoring, FIM, external assessment, malware and card-data discovery, incident, notification, reporting and related compliance features.
Duration	For the term of the relevant service and the deletion period in Section 13, with protected backups expiring no later than 12 months and limited records retained where binding law or a documented legal hold requires.
Nature of processing	Collection, receipt, recording, organisation, structuring, validation, isolation, hashing, scanning, comparison, classification, masking, analysis, correlation, storage, retrieval, consultation, presentation, transmission to Merchant-authorised recipients, restriction, export and deletion.
Purposes	Deliver and secure ThreatView; maintain file-integrity baselines; assess authorised systems; detect malware, exposed card data and payment-page threats; generate findings and PCI DSS evidence; notify authorised recipients; investigate incidents; support the Merchant; maintain availability, auditability and service integrity.
Data subjects	Merchant users, administrators, employees, contractors and service-account holders; merchant customers and website visitors whose data appears in authorised systems or telemetry; incident reporters and affected persons; and other individuals whose data is present in an authorised file, database row, page, log or network transcript.
Personal Data types	Business contact and account data; identifiers and access records; IP addresses, user agents and device data; host, file and database metadata; content and bounded samples; database row context; web, DNS, TLS, HTTP and CSP evidence; screenshots; support and communications; remote-session records; findings, incidents and audit logs; billing references and masked payment-method metadata.
Sensitive or special data	Not intentionally required. Security scans may incidentally encounter special-category data, criminal-offence data, credentials, full PANs or other sensitive content in Merchant-authorised systems. Such data remains subject to the Merchant's instructions and the additional isolation, minimisation, masking and access controls in Schedule 2.
Frequency	Continuous, scheduled, event-driven or on demand, according to enabled features and Merchant configuration.
Merchant instructions	The Agreement, Order, authorised configuration, scope and exclusions, authenticated user actions, approved integrations, support instructions and documented changes.

Schedule 2 Technical and organisational measures

These are the standard measures applied to Merchant Personal Data. They are interpreted with the risk-based qualification in Section 6.

Control area	Standard measure
Governance and accountability	Controlled security and privacy policies; defined service and data ownership; change review; incident, vulnerability and access-management processes; supplier review; records of processing; documented instructions and deletion requests.
Dedicated infrastructure	Backend workloads operate on dedicated servers supplied by Hetzner Online GmbH in German data centres and administered by Turaco. Service roles and trust zones are segmented rather than treated as a flat application network.
Encryption at rest	The primary database volume is encrypted at rest. FIM and external-assessment data drives on dedicated servers are encrypted at rest. Off-site backups stored in Backblaze EU Central, Amsterdam, Netherlands, are encrypted end to end before transfer using keys managed by Turaco, and replication is confined to that region. Backblaze receives no decryption keys and has no access to plaintext Merchant Personal Data within the backup payload. Provider-side account, object, network and operational metadata remains governed and assessed separately.
Encryption in transit	External and service-to-service communications use authenticated encrypted channels appropriate to the protocol. Sensitive remote administration and credential-delivery paths are designed to preserve endpoint identity and confidentiality.
HSM-protected secrets	Stored database, SSH and installation credentials are sealed with AES-256-CCM under a wrap key held inside a hardware security module. The application stores the sealed value and does not receive the wrap key.
Auditable HSM use	Authorised HSM operations use authenticated service identities and capability controls. ThreatView verifies and synchronises the HSM log chain, associates service operations with device entries and fails closed when required audit continuity cannot be established.
Recipient-bound credential release	Supported delivery paths re-wrap an unsealed credential to an ephemeral X25519 recipient key using HKDF-SHA-256 and AES-256-GCM, so intermediaries handle recipient-bound ciphertext rather than a reusable plaintext secret.
Access control	Tenant, group, site and resource scoping; least-privilege service and human roles; authenticated administrative access; session and token controls; MFA or WebAuthn support; access removal and review; auditable privileged actions. Stripe access is separated among account, developer and company-owner roles.
Third-party service credentials	Turaco directly manages the assignment, storage, use and revocation of access keys and other credentials for external services. Credentials are limited to the authorised service purpose and are not embedded in merchant data or disclosed to merchants or unrelated suppliers.
Identity and password protection	Trusted identity is established by the authentication boundary rather than accepted from spoofable client headers. Passwords are protected using randomly salted Argon2id with a separately protected site secret on supported paths, and supported legacy hashes are upgraded through controlled migration.
Workload identity	Sensitive service-to-service, database and message-broker paths use authenticated workload identity and mTLS where configured. HWAUTH-managed certificates bind approved workloads to authorised service identities and lifecycle controls.
Dirty and clean separation	Untrusted content and material that may contain PANs are processed on an isolated dirty side. Validated and minimised results cross to clean services only through bounded interfaces. Dedicated raw card-data analysis uses volatile isolated processing rather than the system of record.

Control area	Standard measure
PAN minimisation	The file-ingestion card-data path validates and masks discovered PANs before clean-side handoff, retaining only limited evidence such as first six, last four, brand and location. Database scanning is separately bounded; ordinary result paths mask PAN matches while configured contextual fields remain protected as sensitive data.
Data minimisation	Hashes, metadata, structured findings and bounded samples are preferred to wholesale content. External assessment retains relevant protocol, HTML, script, screenshot and finding evidence rather than all fetched resources. Queue, cache and deduplication data use bounded lifetimes.
Integrity and traceability	Cryptographic hashes, provenance, timestamps, scope identifiers, change history, request identifiers, delivery status and tamper-evident remote-session transcript chains support verification and investigation.
Availability and recovery	Service health monitoring, protected backups, restoration procedures, capacity controls and incident response support availability and recovery. Backup retention is capped at 12 months. Completed deletion and restriction instructions are reapplied before restored data returns to ordinary processing.
Logging and detection	Authentication, authorisation, API, administrative, HSM, remote-session, service and security events are logged in proportion to risk. Monitoring and alerting support detection, triage, response and forensic preservation.
Employee endpoint security	Phorion provides endpoint detection and response for all employee business-only workstations and several key build servers. Personal devices are not monitored. All EDR features are enabled. Telemetry may include file contents, command lines, URLs, device events and incidental client information, including sensitive information present in monitored material. Additional content filtering or redaction is not applied because it is not feasible for this EDR operation. Data is hosted in the United Kingdom. Only Turaco employees have access to the tenant system and telemetry; supplier access requires Turaco approval and takes place from the United Kingdom. Employees are informed about the monitoring. Telemetry expires seven days after collection, including replicas and backups, and is never exported. Telemetry is used for security, not unrelated purposes. Any processing of special-category or criminal-offence data is subject to the additional conditions required by applicable law.
Secure development and change	Peer review, automated tests, dependency and container controls, controlled deployment, secret separation, least-privilege database roles and security-focused acceptance are applied according to the affected component and risk.
Personnel and confidentiality	Access is limited to authorised personnel bound by confidentiality, with role-appropriate privacy and security instruction and controlled support access.
Deletion and media lifecycle	Authenticated tenant-scoped deletion, reference cleanup, cache/queue expiry and backup expiry are applied according to the store. Memory caches can contain session information and expire within 24 hours. Legal holds are recorded in the database and reviewed at least weekly by system administrators. Deletion resumes automatically when the hold is released. Holds must relate to an applicable obligation or necessary preservation purpose, be limited to relevant records and remain access-restricted. Google Workspace provider recovery/final deletion is separately governed; Phorion telemetry expires within seven days including backups.
Testing and review	Controls are reviewed and tested in proportion to risk through automated testing, operational health checks, security review, incident learning and periodic policy and supplier review.

Schedule 3 Supplier, subprocessor and transfer governance

Turaco maintains confidential supplier and transfer records for governance. The Merchant-facing Supplier and Subprocessor List describes recipients for this core service scope and is maintained at [Turaco Labs Data Processing and GDPR](#). Internal registers do not amend contractual rights merely because an entry changes; Section 7 governs Subprocessor authorisation and notice.

Core service suppliers include Hetzner for dedicated infrastructure in Germany, Backblaze for encrypted backups in EU Central, Amsterdam, Netherlands, Stripe for billing services, and Postmark for email delivery and tracking with three-month message and event retention. Backups are encrypted before transfer using Turaco-managed keys; Backblaze does not receive those keys or plaintext backup contents. Full billing-card information is supplied directly to Stripe, not ThreatView. Google Workspace stores limited business correspondence and contracts. Phorion protects employee workstations and key build servers. Pipedrive supports optional marketing. The legal role of each provider depends on the purpose and data flow.

When a user opts in to ThreatView product updates or communications about other Turaco products and services, Turaco mirrors their name, email address, postal address and telephone number to Pipedrive CRM for marketing and sales management. A threat-alert-only preference does not trigger this transfer. Existing mailbox contents, email bodies and attachments are not mirrored. Pipedrive processes the content of marketing messages sent through its CRM email features and their delivery, open and click events. Every message contains an unsubscribe link. Users may withdraw permission for those emails and their associated tracking by using that link or disabling marketing emails in their Merchant account. Either route stops future Pipedrive marketing messages and tracking and removes the active contact immediately. Contacts are also removed on account deletion or explicit request. There is no separate tracking-only opt-out while continuing to receive Pipedrive marketing emails. Turaco acts as Controller and Pipedrive as its Processor for this purpose. Merchant Security Data is not used for marketing. Primary tenant hosting is in the United Kingdom, with international support and onward processing under the applicable supplier and transfer arrangements.

Google Workspace provides limited business email and document storage. Turaco is Controller for its own correspondence and contracts; Merchant-instruction content remains subject to Subprocessor duties. Emails are deleted once no continuing need exists and on valid request within 30 days unless legally necessary preservation applies. Contracts are typically retained seven years from the end of the relevant financial year. Vault and third-party applications are disabled; three senior employees hold administrator access. Google recovery/final deletion remains separate from active-record purge and platform backup expiry.

Phorion provides endpoint detection and response for all employee business-only workstations and several key build servers. Personal devices are not monitored. All EDR features are enabled. Telemetry may include file contents, command lines, URLs, device events and incidental client information, including sensitive information present in monitored material. Additional content filtering or redaction is not applied because it is not feasible for this EDR operation. Data is hosted in the United Kingdom. Only Turaco employees have access to the tenant system and telemetry; supplier access requires Turaco approval and takes place from the United Kingdom. Employees are informed about the monitoring. Telemetry expires seven days after collection, including replicas and backups, and is never exported. Telemetry is used for security, not unrelated purposes. Any processing of special-category or criminal-offence data is subject to the additional conditions required by applicable law. Merchant-instruction data remains subject to applicable Subprocessor duties.

Support is provided through Turaco-operated RequestTracker 6 on Germany-hosted Hetzner infrastructure. Google reCAPTCHA protects authentication through browser/client collection and a server assessment containing token, site key, user IP, user agent and full request URI; no profile or form content is intentionally supplied. Mapbox receives approximate coordinates, Turaco account token, render parameters and server metadata, not user IP or direct identifiers; images are retrieved and embedded server-side. Standard provider processing and transfer terms govern these limited flows.

Turaco Labs Limited has appointed European Data Protection Office (EDPO), Belgian entity number 0689.629.220, as its Article 27 EU GDPR representative with effect from 2 October 2026. The mandate covers Turaco's Controller and Processor activities governed by EU GDPR, including the EEA. Data Subjects and Supervisory Authorities may contact EDPO in addition to or instead of Turaco at <https://edpo.com/gdpr-data-request/> or by post at Avenue Huart Hamoir 71, 1030 Brussels, Belgium. Niall Newman remains Turaco's Privacy Officer and operational privacy contact.

EDPO handles representative requests and regulatory information and holds Turaco's ROPA governance extract through Imprima. That extract contains no client information or other identifying information. Turaco keeps the complete Article 30 record available to EDPO and competent authorities through its linked records. Representative correspondence and portal account administration may contain the information needed for those functions. EDPO has no routine access to ThreatView databases, FIM content or credentials. Applicable Merchant instructions and the supplier and transfer arrangements govern any disclosure of Merchant Personal Data.

Subprocessor changes and objections follow Section 7. Turaco may withhold supplier pricing, credentials and security-sensitive information while providing the information required by law and this Addendum.

Schedule 4 Execution

This Addendum is ordinarily accepted through an Order. Turaco may also provide an authenticated electronic acceptance route. The signature blocks below may be used where the parties choose to sign.

Merchant	Turaco Labs Limited
Signed for the Merchant	Signed for Turaco Labs Limited
Name	Name: Benjamin Hosack
Title	Title: Chief Executive Officer
Signature	Signature: 
Date	Date: