

THREATVIEW

ThreatView Core Merchant Supplier and Subprocessor List

Recipients purposes and processing locations for core ThreatView services

Document information	Details
Organisation	Turaco Labs Limited; company number 15368842
Registered office	2 Old Bath Road, Newbury, Berkshire, RG14 1QL, United Kingdom
Privacy Officer	Niall Newman; nn@turacolabs.com
Effective and revision date	Effective 6 October 2026; revised 9 October 2026
Version and status	1.4 - effective 6 October 2026; revised 9 October 2026
Responsible executive	Benjamin Hosack, Chief Executive Officer
Classification	Merchant-facing core-service document

Purpose and scope

This list identifies providers used for core ThreatView services and distinguishes Merchant-instruction Subprocessors from suppliers used for Turaco's own business purposes. External partner PCI integration plans are available only to organisations in Australia and New Zealand. European customer organisations have no access to that integration. The additional recipients for those plans require separate programme-specific disclosure and any applicable Merchant authorisation. The providers listed here receive only data relevant to their service and do not all process every Merchant's data. Merchant Security Data is not used for unrelated purposes.

Infrastructure and communications processing

Provider	Purpose and data scope	Main processing location and boundary
Hetzner Online GmbH	Dedicated backend infrastructure including Turaco-operated data, security and support systems; Subprocessor where Merchant Personal Data is hosted	Dedicated infrastructure is hosted in Germany. Hetzner support and administration take place in Germany; authorised Turaco personnel administer servers from the United Kingdom. Platform database volumes and FIM and external-assessment drives are encrypted at rest.
Backblaze, Inc.	Encrypted off-site recovery backups; Subprocessor where the encrypted objects contain Merchant Personal Data	EU Central Amsterdam, Netherlands; region-confined replication. E2E encrypted before transfer with Turaco keys; no plaintext/key access. Maximum 12-month platform backup lifecycle
Postmark operated by AC PM LLC	Email delivery and message events; Subprocessor only where authorised messages contain Merchant Personal Data	United States. Limited message and contact data, with three-month message and event retention. Open and link-click tracking may be disabled separately from necessary delivery records. Tracking redirects may persist longer than event records. Qualifying transfers rely on applicable EU-US Data Privacy Framework and UK Extension adequacy; the account is governed by Postmark's legacy terms.

Limited business and security suppliers

These providers support Turaco's Controller purposes. Where a particular flow processes Personal Data solely under Merchant instructions, the applicable Subprocessor obligations apply.

Provider	Purpose and data scope	Location or processing boundary
Stripe	Payments, Billing, Tax, Subscriptions; billing/transaction information. Card credentials go directly to Stripe, never ThreatView	UK/Irish contractual arrangements with US/global processing under product-specific roles and transfer terms
Pipedrive	Optional ThreatView product-updates and other Turaco products/services marketing: name, email address, postal address and telephone number. A threat-alert-only preference does not trigger transfer. CRM delivery, open and click events support aggregate marketing statistics. Unsubscribing or disabling marketing in the account stops future marketing emails and associated tracking and removes active contacts immediately. Contacts are also removed on account deletion or explicit request. No separate tracking-only opt-out is available.	UK primary tenant storage; US/global support and onward processing under applicable DPA, adequacy and transfer safeguards. Provider recovery/backups expire separately from active removal.
Google Workspace	Email/contracts containing limited client information. No Vault or third-party apps; three senior administrators	International standard provider processing; Starter has no selectable region policy. Active purge separate from Google recovery/final deletion
Phorion Technology Ltd	EDR for all business-only employee workstations and key build servers; no personal devices. Content, commands, URLs and incidental client information may be captured. Sensitive data is not deliberately sought; no additional content minimisation is feasible for the EDR operation.	UK hosting; approved supplier access from the UK; employee tenant access. Seven days from collection including replicas/backups; no telemetry exports
Google reCAPTCHA Enterprise	Authentication protection through browser/client and limited server token, site-key, IP, user-agent, URI assessment	Google standard Cloud processing; security cookie/browser technical information and applicable international safeguards
Mapbox	Server-rendered static security maps using rough coordinates, account token and server request metadata	No end-user IP or direct merchant/person identifier supplied; covered API/request data processed under the current DPA, with separate account purposes. US/international handling with qualifying DPF and contractual safeguards.
European Data Protection Office	EU Article 27 representative; necessary request and regulatory records and Turaco's ROPA governance extract	Belgium; qualifying exchanges with the United Kingdom use applicable adequacy arrangements. The Imprima ROPA extract contains no client information or other identifying content. Representative correspondence and portal account administration are processed separately.

Subprocessor changes and objections

Turaco gives affected Merchants at least 30 days' advance email notice of an intended Subprocessor addition or replacement under general authorisation. A Merchant may object on reasonable, documented data-protection grounds by emailing support@turacolabs.com. Turaco seeks additional safeguards or another reasonable solution. If the objection cannot be resolved, the affected Merchant may close the account before the change takes effect.

Provider roles depend on the purpose, contract and data flow. Restricted Transfers require applicable adequacy or contractual safeguards and the relevant risk assessment. Further information is available from Niall Newman, Privacy Officer, at nn@turacolabs.com. Detection rules, keys and confidential risk assessments are not published.