

THREATVIEW

Privacy Notice and Data Protection Complaint Procedure

How Turaco Labs uses personal data as controller and how to make a data protection complaint

Document information	Details
Controller	Turaco Labs Limited
Company	Company number 15368842; incorporated in England and Wales
Parent holding company	Turaco Labs, company number C204814 GBC, registered at AMG Services Ltd, 11th Floor, Tower A, 1 Exchange Square, Ebene, Mauritius
Registered office	2 Old Bath Road, Newbury, Berkshire, RG14 1QL, United Kingdom
Effective date	6 October 2026
Version and status	1.5 - effective 6 October 2026; revised 12 October 2026
Review cycle	At least annually and whenever purposes, suppliers, law or material processing changes
Privacy Officer	Niall Newman - nn@turacolabs.com
Data protection complaints	support@turacolabs.com
Responsible executive	Benjamin Hosack, Chief Executive Officer

Scope of this Notice

This Notice explains Turaco Labs Limited's use of Personal Data for core ThreatView accounts, security, billing, support, correspondence and optional marketing, and the privacy rights and complaint routes available to individuals. External partner PCI integration plans are available only to organisations in Australia and New Zealand. European customer organisations have no access to that integration. That additional processing requires separate programme-specific privacy disclosures.

Contents

- 1 Purpose scope and roles
- 2 Who we are and how to contact us
- 3 Personal data we collect
- 4 Where personal data comes from
- 5 Purposes and lawful bases
- 6 Data you must provide
- 7 Recipients and disclosures
- 8 International transfers
- 9 Retention and deletion
- 10 Security
- 11 Your rights
- 12 Automated processing
- 13 Children
- 14 Marketing cookies and communications
- 15 Data protection complaint procedure
- 16 Changes to this Notice

A reference to you includes a person acting with proper authority for an individual. Rights and complaint routes are available without the need to quote legislation or use a prescribed form.

1 Purpose scope and roles

This Privacy Notice explains how Turaco Labs Limited collects and uses personal data when it acts as a Controller. It applies to visitors to our websites, prospective and current customers, ThreatView users and administrators, billing and business contacts, people who contact support, and people who make privacy requests or complaints.

ThreatView is a business security monitoring, assessment and PCI DSS support service. It is not directed at consumers or children.

Turaco also processes some data on a merchant's behalf. When a merchant chooses the websites, systems, files, databases, logs or other assets monitored through ThreatView, the merchant is normally the Controller of Personal Data in those assets and Turaco is its Processor. That activity is governed by the merchant's instructions, the ThreatView Merchant Data Processing Addendum and the Merchant Data Processing Policy. The merchant's privacy information explains why the merchant processes that data.

This Notice does not convert merchant-controlled data into Turaco-controlled data and does not authorise Turaco to use Merchant Security Data for unrelated purposes. If a Merchant is itself a Processor, Turaco may act as its Subprocessor for the instructed service.

Context	Usual role
ThreatView user accounts, authentication, platform administration and service communications	Turaco as Controller
Billing, invoicing and Turaco transaction records	Turaco as Controller; Stripe's role depends on the relevant payment service and its current terms
Turaco platform security, abuse prevention, audit and legal records	Turaco as Controller
FIM, external assessments, database or file scanning, browser or payment-page monitoring and merchant findings	Merchant as Controller; Turaco as Processor
Merchant-selected identity provider, webhook, partner or other destination	Role determined by the Merchant's instruction and the recipient's actual purposes and terms
Authorised personnel including directly engaged contractors	When acting within their authorised duties and under Turaco Labs Limited's direct authority and documented instructions, they are part of Turaco's personnel arrangements for the relevant processing activity rather than a separate organisational Controller or Processor.

2 Who we are and how to contact us

Turaco Labs Limited is incorporated in England and Wales under company number 15368842. Our registered office is 2 Old Bath Road, Newbury, Berkshire, RG14 1QL, United Kingdom.

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 does not receive Personal Data through that ownership relationship or Turaco's personnel arrangements. Turaco Labs Limited remains the contracting entity for ThreatView and the Controller responsible for the processing described in this Notice.

For the Controller processing described in this Notice, Turaco is responsible for deciding why and how Personal Data is used. Privacy questions and rights requests may be sent to Niall Newman, our Privacy Officer, at nn@turacolabs.com, or by post to our registered office. Data protection complaints may be sent to support@turacolabs.com.

Turaco is not required to appoint a statutory Data Protection Officer. Niall Newman is our Privacy Officer and coordinates privacy governance, rights requests and complaint oversight. We review the need for a statutory DPO if our processing materially changes.

ThreatView is offered directly throughout the European Economic Area. With effect from 2 October 2026, Turaco Labs Limited has appointed European Data Protection Office (EDPO), a Belgian public limited liability company registered under number 0689.629.220, as its representative under Article 27 EU GDPR. 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 United Kingdom Privacy Officer. EDPO's representative role is separate from that role and is not a DPO appointment.

EDPO's appointment certificate was issued on 2 October 2026 and is valid until 1 October 2027, conditional on Turaco maintaining the appointment. It evidences Article 27 representation, not certification of overall GDPR compliance. View the publicly published appointment certificate.

3 Personal data we collect

Category	Examples
Identity and business contact	Name, organisation, job title, username, business email, telephone number, postal and billing address.
Account and profile	Tenant and account identifiers, roles, permissions, account state, preferences, accepted terms and user-selected settings.
Authentication and security	Password hashes, MFA/WebAuthn and SSO information, sessions/tokens, access outcomes, source IP/user agent and approximate location. Business-workstation and build-server EDR may incidentally collect client information in file contents, command lines and URLs under the separate security purpose.
Technical and usage	IP address, browser and operating-system details, page and feature use, API activity, timestamps, request identifiers, service and error logs.
Billing and transaction	Billing contact, tax and invoice information, plan and entitlement, Stripe customer, invoice, payment-method and subscription identifiers, payment status and Stripe-returned masked payment metadata.
Support and communications	Requests and correspondence held in Turaco's self-hosted Request Tracker 6 system; attachments and troubleshooting material; email recipient and sender data; message content; delivery and bounce events; and Postmark open and link-click events for service and marketing messages. Emails may contain a person's name, company name and registered domain. Google Workspace business email may contain limited client information in correspondence, separate from the ThreatView notification archive and Postmark tracking.
Marketing and preference	Marketing choices made during signup, subscription state, subsequent preference changes and opt-out records; interaction information only where lawfully collected. For the Pipedrive contact workflow, the mirrored fields are name, email address, postal address and telephone number.
Privacy complaint contractual and legal records	Rights requests, complaints, proportionate identity or authority evidence, investigation records, outcomes, legal correspondence and records held for claims or compliance. Limited client information may also appear in contractual documents stored in Google Workspace for relationship administration and accounting.
Derived and automated security decision data	Service-use statistics, access and system-usage signals, suspected-abuse indicators, automated restriction or suspension outcomes and operational measures that remain Personal Data unless irreversibly anonymised.

Billing card data

Payment card details used to pay Turaco are entered into and processed directly by Stripe. ThreatView does not receive or store the full card number, card verification code, PIN data or magnetic-stripe data for billing. Turaco receives the billing identifiers, payment status, invoice information and limited masked metadata needed to administer the service, such as card brand, expiry and last four digits where Stripe returns them.

ThreatView security features may separately encounter payment-card information in a merchant-controlled system when the merchant instructs ThreatView to perform card-data discovery. That is Processor activity governed by the Merchant's instructions and Data Processing Addendum, not Turaco's billing activity.

Sensitive data

Turaco does not ask users to provide special-category Personal Data or criminal-offence data for ordinary account, billing or support purposes. Please do not include unnecessary sensitive information in free-text fields, support messages or complaints. If it is necessary to investigate a request or legal matter, Turaco will use the information only where a valid additional legal condition applies and will restrict access accordingly.

4 Where personal data comes from

We collect Personal Data from the following sources:

- directly from you when you create or use an account, contact us, purchase a service, configure preferences, exercise a right or make a complaint;
- from the Merchant or organisation that creates, sponsors or administers your ThreatView account;
- from your identity provider when your organisation uses enterprise SSO;
- automatically from your browser, device and interactions with ThreatView, including through essential cookies and service logs;
- from Stripe in connection with billing and subscription administration;
- from Postmark in connection with email delivery, bounce, open and link-click tracking; from Google reCAPTCHA Enterprise during authentication; from Mapbox in connection with authentication-related security messaging; and from the relevant service records generated by those integrations;
- from a person authorised to act on your behalf;
- from device-security telemetry generated on Turaco employee workstations and processed through Phorion where limited client information appears incidentally;
- from professional advisers, public authorities or public corporate sources where necessary to verify information, comply with law or manage legal claims; and
- from service records generated when we provide, secure and support ThreatView.

Where we obtain Personal Data from another source, we provide the applicable privacy information within the period required by law, ordinarily no later than one month and, where relevant, by the first communication or disclosure, unless a lawful exception applies.

5 Purposes and lawful bases

Purpose	Data	Lawful basis and interest
Create and administer Merchant and user accounts	Identity, contact, account and profile	Legitimate interests in delivering and administering a contracted business service; contract where the individual is personally party to it.
Authenticate users, manage sessions, enforce permissions and respond to serious abuse	Identity, account, authentication, access logs, system usage and technical data	Legitimate interests in protecting ThreatView, Merchants and users; contract where applicable. Significant automated decisions are subject to the safeguards described in Section 12 and any applicable EU GDPR restriction.
Provide service and business communications and administer contracts	Identity, business contact, account, communications and relevant contractual records	Contract where applicable; otherwise legitimate interests in operating the service and relationship.
Administer subscriptions, invoices, payments, debt recovery and accounting records	Identity, business contact, billing, transaction and relevant contractual records	Contract where applicable; tax and accounting legal obligations where they apply; otherwise legitimate interests in necessary accounting and evidential records, receiving payment and preventing fraud.
Provide support and resolve faults	Identity, contact, account, technical and communications	Contract where applicable; legitimate interests in support, reliability and issue resolution.
Protect ThreatView and investigate abuse or security events	Authentication, technical, usage, audit and communications data; limited client Personal Data incidentally included in business-workstation and build-server security telemetry.	Legitimate interests in network and information security, fraud and abuse prevention, incident response and legal claims; legal obligation where applicable.
Maintain auditability and demonstrate compliance	Account, authentication, technical, complaint and legal	Legal obligation; legitimate interests in accountability, evidential integrity and legal claims.
Handle privacy rights and complaints	Identity, contact, account, complaint and legal	Legal obligation; legitimate interests in investigation, remediation and accountable records.
Improve reliability and user experience	Usage, technical, support and aggregated measures	Legitimate interests in maintaining and improving the service, using minimised or aggregated data where practicable.
Optional Pipedrive marketing and sales management	Name, email address, postal address and telephone number; signup marketing choice and subsequent preferences	Consent for this optional signup-based marketing and contact-management purpose. You may withdraw at any time. Withdrawal stops this marketing use and does not affect the lawfulness of prior processing or essential account communications.

Purpose	Data	Lawful basis and interest
Other permitted marketing and email delivery or interaction measurement	Identity, contact, preference, delivery, open and link-click information where lawfully collected	Consent for optional signup-based marketing. Contract or legitimate interests, where applicable, for necessary delivery and abuse prevention. Open and link-click tracking is subject to any separate permission required by applicable electronic-privacy law.
Operate non-essential analytics or similar technologies	Technical and usage	Consent where required by PECR.
Obtain professional advice, meet Turaco Labs Limited's corporate-governance and legal obligations, respond to lawful requests and manage corporate change	Relevant minimum categories	Legal obligation where applicable; otherwise legitimate interests in professional advice, corporate governance, accountability, continuity and legal claims, subject to a documented necessity and balancing assessment.

Where we rely on legitimate interests, we consider the specific purpose, necessity and effects on individuals. The stated interests are necessary business administration, proportionate security, reliability, accountability and relevant legal claims. They do not authorise unrelated use of Merchant Security Data or replace consent or other conditions where law requires them.

Where we rely on consent, consent may be withdrawn at any time without affecting processing carried out before withdrawal. We do not sell Personal Data and do not disclose Merchant Security Data to advertising networks or data brokers.

6 Data you must provide

Identity, business contact, authentication and account data marked as required is necessary to create, administer and secure a ThreatView account. Billing information is necessary where you or your organisation purchases a paid service. If required data is not provided, we may be unable to create the account, provide the requested service, process the purchase or investigate a request.

Marketing choices are optional. Opting out does not stop service, billing, account or security communications necessary to administer or secure the account.

A privacy complaint does not need legal language or a prescribed form. We may need enough information to understand the concern, verify identity proportionately or confirm a representative's authority. A lack of relevant information may limit what we can investigate.

7 Recipients and disclosures

We disclose only the Personal Data reasonably necessary for the stated purpose. Depending on the service and options in use, recipients may include:

- the Merchant organisation responsible for your account and its authorised administrators;
- dedicated infrastructure, encrypted-backup, payment, communications, business email and document storage, marketing and sales CRM, employee endpoint-security, authentication, anti-abuse and EEA representative suppliers operating under appropriate contractual and security controls;
- Stripe for direct payment processing and subscription administration;
- Postmark for transactional email delivery and message-event tracking;
- Google reCAPTCHA Enterprise for authentication abuse prevention. ThreatView's server-side assessment sends Google a reCAPTCHA token, site key, the user's IP address and browser user agent, and the full authentication request URI, which may contain a workflow identifier. ThreatView does not intentionally submit account-profile or form-field content. The reCAPTCHA client also communicates directly between the user's browser and Google;
- Mapbox for authentication-related static security maps. ThreatView sends approximate IP-derived longitude and latitude, a Mapbox access token, fixed rendering parameters and server connection metadata. It does not send the user's source IP, identity, email address, browser user agent, account or Merchant identifier, or event identifier. ThreatView retrieves and embeds the image server-side, so the recipient does not load the image from Mapbox;
- an identity provider, webhook, partner portal or other destination selected by the Merchant;
- professional advisers, insurers, auditors and prospective parties to a reorganisation, sale or acquisition, subject to confidentiality and safeguards; and
- courts, regulators, law-enforcement bodies or other competent authorities where disclosure is required or permitted by law.

Where the disclosed Personal Data is processed by Turaco Labs Limited as Controller, Turaco remains responsible for the processing described in this Notice. Access by authorised employees and directly engaged contractors is limited to their duties under Turaco's authority and applicable confidentiality, security, privacy and access-control procedures.

Core service providers include Hetzner Online GmbH for dedicated infrastructure, support and administration in Germany; Backblaze, Inc. for end-to-end encrypted backups in EU Central, Amsterdam, Netherlands; Stripe Payments, Billing, Tax and Subscriptions; Postmark for email delivery and three-month message and event retention; Google reCAPTCHA Enterprise for authentication protection; and Mapbox for server-rendered static security maps using approximate coordinates without direct user or Merchant identifiers. Backblaze does not receive Turaco's decryption keys or plaintext backup contents. Support is provided through Turaco's self-hosted Request Tracker 6 on Hetzner infrastructure.

Pipedrive processes optional marketing and sales contact records and the email content and events generated through its CRM features. This is separate from the Merchant security repository. Only the two marketing choices specified in Section 14 trigger mirroring. The primary tenant is hosted in the United Kingdom; international support and onward processing follow the applicable supplier terms.

We use Google Workspace for business email and documents containing limited client information, including correspondence and contracts. Google processes stored content on our behalf; its account and service data have separate terms. This is not a general Merchant Security Data repository. Vault is not enabled, administrators are limited to three senior employees and no third-party applications are enabled. Business email follows our existing archive policy; contracts are usually retained for seven years from the end of the relevant financial year. Google-controlled recovery and final deletion have a separate lifecycle from removal of active Turaco records.

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.

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. Disclosure is limited to the representative function and legal requirements. Return, deletion and legally required retention are governed by the mandate.

Turaco maintains supplier roles and transfer information in its internal records. The Merchant-facing Supplier and Subprocessor List describes recipients for the applicable service scope. Confidential risk assessments and detection rules are not published, but relevant information remains available for lawful assurance and rights requests.

8 International transfers

Some suppliers or Merchant-selected destinations process Personal Data outside the UK. Hetzner hosting and provider infrastructure support/administration are confined to Germany; Turaco personnel administer the service from the UK; Backblaze encrypted backup storage/replication to Amsterdam with no provider plaintext/key access. Stripe uses UK, Irish and international arrangements; Postmark processes in the US; Google and Pipedrive can use international processing. Mapbox receives limited server-side mapping inputs, not end-user IPs or direct identifiers. Qualifying EEA-to-UK transfers use the applicable European Commission UK adequacy decision while it remains valid; this is separate from Turaco's Article 27 representative appointment.

EDPO is established in Belgium and receives information needed for the representative function. Qualifying transfers between the United Kingdom and the EEA rely on the applicable adequacy arrangements. The ROPA governance extract held through Imprima contains no client information or other identifying content. Necessary representative correspondence and portal account information are processed separately.

Pipedrive's primary tenant is hosted in the United Kingdom. Its DPA permits United States and other international support and onward processing, subject to the applicable adequacy and contractual safeguards. Provider recovery and backup copies expire separately from active-contact removal.

Google Workspace does not provide selectable data-region policies. Content, support and service processing may involve international locations under Google's standard processing and transfer terms.

Phorion data is hosted in the United Kingdom. Supplier access requires Turaco approval and takes place from the United Kingdom. Telemetry expires seven days after collection, including replicas and backups. Turaco assesses any new overseas recipient or access route before permitting it.

Qualifying transfers rely on applicable United Kingdom or European Union adequacy arrangements, including the EU-US Data Privacy Framework and UK Extension for covered entities and data. Other Restricted Transfers require a valid transfer mechanism and the relevant risk assessment. Encryption protects confidentiality but does not replace a required legal transfer mechanism.

You may request information about the safeguard relevant to your Personal Data by contacting nn@turacolabs.com. We may redact confidential or security-sensitive material while still providing a meaningful description of the protection.

9 Retention and deletion

We keep Personal Data only for as long as needed for the collection purpose, taking account of amount, nature and sensitivity, security and evidential needs, legal and regulatory duties, limitation periods and whether the purpose can be achieved using less data.

Niall Newman, Privacy Officer, maintains Turaco's retention schedule. Legal holds are recorded in the database and reviewed at least weekly by system administrators. A hold is limited to relevant records needed for an applicable obligation or preservation purpose, and access remains restricted. Deletion resumes automatically when the hold is released. We notify affected users of legal requests where lawful and practicable, unless notice would prejudice an investigation or create a security risk.

Record type	Retention rule
Account and service administration	For the active relationship. A closed account without a deletion request may be retained for reactivation for up to two years after closure. Following a valid deletion request, live account data is deleted within 30 days, subject to legal retention and documented holds. Merchant-controlled raw content follows the DPA and documented instructions, rather than the closed-account retention period.
Contractual documents	Relevant contractual documents are typically retained for seven years from the end of the relevant financial year for accounting and evidential purposes. A longer period applies only where an applicable legal requirement or documented hold makes it necessary.
Invoices tax and other accounting records	Up to six years after the relevant relationship or accounting period where required or reasonably necessary, and longer only where law or a documented legal hold requires. Contractual documents follow the separate typical seven-year rule above.
Authentication API security and administrative logs	90 days, unless a documented legal hold or incident-preservation requirement requires longer retention of relevant records.
Phorion employee-workstation and build-server telemetry	Seven days from collection, including replicas and backups. No telemetry is exported. Platform logs and separate incident records follow their own retention periods.
HSM credential and security audit metadata	HSM device audit metadata contains no identifying information and is retained for security integrity. Separate attributable application/security logs follow their applicable 90-day rule unless necessary preservation applies.
Security incidents and remote-session records	Incident and remote-session records are anonymised for operational record keeping and to document actions in Merchant environments. Account identifiers are removed. Ambiguous recording content receives human review to remove Personal Data, and retained internal links do not identify an account or individual. Identifiable evidence is retained only while needed for a specific incident, claim, legal obligation or documented hold, and is then deleted. Only records that cannot reasonably identify or be relinked to a person are retained indefinitely.
ThreatView notification archive and Postmark copies	ThreatView notification records have no fixed expiry while needed for communications, accountability or legal purposes. They are deleted when no continuing need exists. On a valid deletion request, active content and associated identifying metadata are deleted within 30 days unless applicable law or a documented hold requires preservation. Postmark retains message and event copies for three months; tracking redirects may persist longer than the event records.

Record type	Retention rule
Google Workspace business email	Business email has no fixed expiry. Identifiable records are retained while needed for the current relationship, unresolved support or complaints, an identified abuse-prevention need, a legal obligation or a specific claim or dispute. Records and associated identifying metadata are deleted when no continuing need exists, unless a documented legal hold applies. Continuing necessity is reviewed at least annually and when a purpose or hold ends. Valid requested active-record deletion takes place within 30 days, subject to applicable law and documented holds. Google-controlled recovery and final deletion follow the provider's separate lifecycle. Google Vault is not enabled.
Request Tracker tickets and attachments	Tickets and attachments are held in an employee-only, self-hosted support system and are linked to accounts for deletion. Identifiable records are retained while needed for the current relationship, unresolved support or complaints, an identified abuse-prevention need, a legal obligation or a specific claim or dispute. Records and associated identifying metadata are deleted when no continuing need exists, unless a documented legal hold applies. Continuing necessity is reviewed at least annually and when a purpose or hold ends. Valid requested active-record deletion takes place within 30 days, subject to applicable law and documented holds.
Privacy requests and complaint files	Identifiable records are retained while needed for the current relationship, unresolved support or complaints, an identified abuse-prevention need, a legal obligation or a specific claim or dispute. Records and associated identifying metadata are deleted when no continuing need exists, unless a documented legal hold applies. Continuing necessity is reviewed at least annually and when a purpose or hold ends. Valid requested active-record deletion takes place within 30 days, subject to applicable law and documented holds.
Enquiries prospects marketing history and preferences	Enquiry, prospect and marketing history is retained for up to 12 months from the end of the relationship. Minimal suppression information is retained only while necessary to honour an opt-out and is not used for marketing. Active Pipedrive contacts are removed immediately on marketing withdrawal, email opt-out, account deletion or explicit request. Provider recovery and backup copies expire separately under the provider terms.
Payment and subscription metadata	Accounting and tax records follow the six-year retention rule above. Other payment and subscription records follow the continuing-need criteria, annual review, 30-day requested deletion and lawful preservation exceptions described for privacy requests and complaint files.
FIM baselines and version history	Retained for the active service without a fixed expiry and deleted from live systems within 30 days of a valid account-deletion request, subject to legal retention and backup expiry within 12 months.
Database query results and row context	Retained for the active service without a fixed expiry and deleted from live systems within 30 days of a valid account-deletion request, subject to legal retention and backup expiry within 12 months.
External-scan evidence	Public-source security evidence may be retained without a fixed expiry while needed for its security purpose. A person whose Personal Data appears in a scan may request deletion of the scan and associated data under the normal rights and deletion process.
Browser and CSP telemetry	13 months, with live data deleted within 30 days of a valid account-deletion request where applicable, subject to legal retention.
Availability-monitoring history	Four years, with live data deleted within 30 days of a valid account-deletion request where applicable, subject to legal retention.
Queues retries and dead letters	No more than 24 hours.

Record type	Retention rule
Caches sessions and temporary keys	Memory caches may contain session information. Contents expire within a maximum of 24 hours and are not a permanent system of record.
Object-store material and encrypted backups	Object-store material is retained for the active service without a fixed expiry and deleted within 30 days of a valid account-deletion request, subject to any shorter category rule and legal retention. Encrypted backup copies expire within 12 months and prior deletion instructions are reapplied after restoration.

If a Turaco platform backup containing data previously deleted from live systems is restored, deletion instructions are reapplied before ordinary service resumes unless a documented legal obligation requires otherwise. Google Workspace recovery and provider backups follow Google's separate lifecycle.

10 Security

Turaco applies technical and organisational measures proportionate to the sensitivity of Personal Data and processing risks. These include dedicated backend servers, encrypted data volumes and backups, encryption in transit, service authentication, network segmentation, least-privilege access, tenant isolation, protected content-processing boundaries, security logging and monitoring, backup and incident-response procedures, and confidentiality duties for authorised personnel. Directly engaged contractors working under Turaco's direct authority follow the same applicable procedures as equivalent employees. The UK-based core developer uses a dedicated machine only for Turaco Labs Limited operations and maintains strict separation from parent-company systems and activities. Turaco manages external-service access keys directly. Stripe access is separated among account, developer and company-owner roles.

Sensitive stored database, SSH and installation credentials are sealed under hardware security module protected keys. Security-relevant HSM use is associated with an auditable operation record and supported credential-delivery paths use recipient-bound encrypted transport. The detailed controls and cryptographic design are documented in the technical and organisational measures annex to the ThreatView Merchant Data Processing Addendum.

No method of storage or transmission eliminates every risk. Turaco reviews controls in light of service changes and identified threats and will notify regulators and affected people where law requires.

11 Your rights

Depending on the circumstances and applicable exemptions, you may have the right to:

- be informed about use of your Personal Data;
- obtain access to your Personal Data and supplementary information;
- have inaccurate data corrected and incomplete data completed;
- request erasure;
- request restriction of processing;
- receive qualifying data in a structured, commonly used and machine-readable format and have it transmitted to another Controller;
- object to processing based on legitimate interests;
- object at any time to direct marketing;
- withdraw consent where consent is the lawful basis; and
- complain to Turaco and the Information Commissioner's Office.

Rights are not absolute. If an exemption applies or we need to retain information for law or legal claims, we will explain the position unless law prevents us from doing so. We do not normally charge a fee; we may charge a reasonable fee or refuse only where law permits, including for a manifestly unfounded or excessive request.

We may request information reasonably needed to confirm identity or authority but will not ask for additional identity evidence where already satisfied. We respond without undue delay and ordinarily within one calendar month after receiving the request and any reasonably required identity information. Where law permits an extension for complexity or multiple requests, we will notify you within the initial period and explain why.

If your request concerns Personal Data in a Merchant-controlled monitored system, the Merchant is normally responsible. You may contact the Merchant directly. If Turaco receives the request, we will identify the appropriate Controller where reasonably possible, forward the request securely and assist the Merchant under the Data Processing Addendum. We will not independently disclose Processor-held Merchant Data without the Merchant's instruction unless law requires it.

12 Automated processing

ThreatView uses automated tools to identify security events, calculate system-security scores, classify findings, detect suspected abuse and prioritise investigation. These outputs concern systems, accounts and security events.

Serious suspected compromise or misuse can automatically block the whole account at login. Some blocks expire at a preset time; others may remain indefinitely. The initial block is imposed without human intervention. Notice is provided by email or during sign-in. Human review takes place only if an appeal is made.

You may appeal by emailing support@turacolabs.com, explaining your views and contesting the restriction. An authorised human reviewer handles the appeal within one business day and can overturn the block. There is no proactive or periodic human review. Applicable statutory rights concerning automated decisions remain available.

13 Children

ThreatView is a business service and is not intended for children. Turaco does not knowingly invite children to create ThreatView accounts.

Merchant-controlled systems monitored through ThreatView may contain information relating to children. In that context the Merchant determines the purpose and lawful basis and Turaco acts only on its instructions.

Children have data-protection rights. If a child makes a complaint or request, we will communicate in clear age-appropriate language, assess competence and authority proportionately, and prioritise information indicating an urgent safeguarding concern.

14 Marketing cookies and communications

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. Withdrawal does not stop essential service, billing, account or security messages. We do not share contacts for another organisation's own marketing without the appropriate permission.

ThreatView uses cookies and similar technologies necessary for authentication, security, preferences and service operation. Google reCAPTCHA uses the _GRECAPTCHA risk-analysis cookie and browser technical information; its use of Google domains may also interact with pre-existing Google cookies. ThreatView sends the limited server assessment fields described above. No separate advertising or analytics technology is currently enabled. Any new non-essential technology must be disclosed and used only with the permission required by applicable electronic-privacy law.

Postmark delivers service and permitted marketing messages and records delivery and bounce events. Optional open and link-click tracking creates a communications history that Merchants can view in their account. You may opt out of Postmark open and link tracking through the tracking preference or support@turacolabs.com. This stops those measurements in future messages, but not necessary delivery and bounce records. An open event is a technical signal, not proof that a person read an email. Postmark message and event copies are retained for three months. Pipedrive CRM separately measures delivery, open and click rates for aggregate marketing statistics. Its tracking stops when you unsubscribe from marketing emails or disable marketing in your account; either route removes the active contact immediately. Pipedrive does not provide a tracking-only opt-out while continuing those emails. Tracking remains subject to any prior permission required by applicable law.

15 Data protection complaint procedure

How to complain

You may complain if you believe Turaco has infringed data-protection law in the way it collected, used, stored, shared or secured your Personal Data, or responded to a request about it.

Send complaints to support@turacolabs.com with the subject Data Protection Complaint, or write to our registered office. You may also contact Niall Newman, Privacy Officer, at nn@turacolabs.com. You may use another available contact route and do not need to quote legislation or use a prescribed form. We will accept and route a complaint received through any Turaco channel. For matters governed by EU GDPR, you may also contact EDPO using the representative contact details in Section 2. Contacting EDPO is an alternative route, not a prerequisite to contacting Turaco or a Supervisory Authority.

Please describe what happened, the Personal Data or account involved, the outcome sought and information that may help us investigate. Do not send unnecessary identity documents or sensitive information unless we ask for them through an appropriate channel.

Representatives and identity

A person may complain for someone else. We ask for proportionate evidence of authority, such as signed authority or an appropriate power of attorney. If we reasonably doubt identity, we request the minimum additional evidence needed promptly and securely. We do not disclose Personal Data to an unauthorised representative, but may take immediate action needed to contain a security risk.

Acknowledgement

We acknowledge receipt within 30 days, provide a reference or contact point where practicable and explain the next step. Investigation begins on receipt, and separate information-rights requests remain subject to their statutory deadlines.

Investigation

Without undue delay, we take steps appropriate to the circumstances. This may include clarifying the issues and requested outcome, examining relevant records, comparing the complaint with information we hold, speaking to relevant personnel, checking contracts, policies and controls, and obtaining information from a Processor, supplier or Merchant Controller.

We investigate thoroughly, fairly and accurately while avoiding unnecessary or disproportionate access to Personal Data. We take account of complexity, scale, current harm and any urgent security or safeguarding concern.

Where the complaint concerns Merchant-controlled data, we securely forward it to the Merchant Controller and provide assistance required by the Data Processing Addendum. If the complaint also concerns Turaco's Controller processing, we handle that aspect directly.

Progress updates

We keep the complainant informed without undue delay. If an investigation cannot be completed promptly, we explain expected timing, identify a contact point and provide further updates when timing changes or a material development occurs.

Outcome

We communicate the outcome without undue delay after completing the investigation. The response addresses the material points, explains the enquiries and reasons for the conclusion, and identifies any correction, deletion, restriction, security improvement or other remedial action where appropriate.

If we conclude that our processing complied with the law, we explain the basis sufficiently for the complainant to understand it. Where another person's rights, confidentiality, legal privilege or another lawful restriction prevents disclosure, we explain the position to the extent permitted.

Escalation

You may complain to the Information Commissioner's Office at any time and do not have to wait for Turaco's process to finish. We welcome the opportunity to investigate first, but this does not restrict your right to contact the ICO or seek a judicial remedy. If another Supervisory Authority is competent under applicable law, you may also complain to that authority.

[Information Commissioner's Office complaint service](#)

Complaint records and improvement

We keep access-restricted complaint records to investigate and document our response, address an identified abuse risk, comply with applicable law or handle a relevant claim or dispute. Records are deleted when no continuing need exists. Valid

requested deletion takes place within 30 days, subject to lawful preservation exceptions. We review complaint themes and outcomes to improve handling.

16 Changes to this Notice

We review this Notice regularly and update its version and effective date when processing, suppliers, law or controls change. Where a change materially affects an individual or introduces a new purpose, we bring it to affected people before the new processing begins where law requires.