

PAPER TIGER TECHNOLOGIES

Privacy Policy

1. Purpose

The purpose of this Privacy Policy is to describe, for the fictional PaperTiger service, what personal data would be collected, why it would be used, and the choices available to individuals. It is an illustrative privacy notice, not a statement about any real service.

Privacy is a trust expectation as much as a legal topic: people want to know what is collected about them and what they can do about it. This policy lays out the collection, use, retention, and choice model in plain language so the demonstration reads like a real, mature privacy notice.

This policy is fictional and illustrative. It describes no real data subject, collection, or processing.

The policy is written in plain language because the audience is the individual whose data is at issue, and a notice that requires legal expertise to understand fails its own purpose.

Privacy is kept by matching what the notice promises to what the organization actually does, so the policy spends its effort on purpose, minimization, and delivering on rights.

Privacy lives or dies on whether the notice matches reality, so the policy drives consent, impact assessment, and sharing limits to keep the two aligned.

The privacy policy exists to show how a real organization states its handling of personal data, in original wording and marked fictional throughout.

2. Definitions

Term	Definition (illustrative)
Personal data	Information relating to an identified or identifiable individual.
Controller	The party that decides the purposes and means of processing.
Processor	The party that processes personal data on the controller's behalf.
Data subject	The individual to whom personal data relates.
Data subject request	An individual's request to access, correct, or delete their data.
Processing	Any operation on personal data, such as collection, storage, or use.
Retention	The period personal data is kept before

	deletion.
Choice	The options available to an individual about their data.
Vendor records	The supplier and vendor information a customer submits.
Legal basis	The illustrative justification for a processing activity.
Privacy review	The pre-launch assessment of new processing.
Data portability	The right to obtain data in a usable format.
Privacy training	The role-specific instruction for data handlers.
Processing purpose	The stated reason personal data is collected and used, which bounds what may be done with it.
Consent	The illustrated individual's agreement to a specific processing purpose.
Data protection impact assessment (DPIA)	The structured review of a processing activity's privacy risk before it is introduced.
Record of processing activities	The maintained list of what personal data is processed, why, and by whom.
Privacy notice	The plain-language description of how the demonstration handles personal data.
Record of processing	The maintained list of what personal data is processed, why, and by whom.
Lawful basis	The stated reason a processing activity relies on in the fiction.
Right to erasure	The right to have personal data deleted.
Privacy by design	The embedding of privacy into a system from the start.
Data protection	The safeguards applied to personal data.
Transfer review	The check of a cross-border transfer and its basis.

3. Scope and Boundaries

This policy applies to fictional personal data processed in connection with the illustrated service, including data submitted by customers about their vendors. It covers collection, use, sharing, retention, and individual rights.

It applies to personal data in any format or location within the service boundary, regardless of who supplied it.

Out of scope are real personal data and real processing. This policy creates no real legal obligation.

The scope includes personal data in any format or location, so a data subject's rights do not depend on where their data happens to be stored.

Escalation for a privacy issue follows a fixed chain: a concern goes to the privacy owner, then to the Information Security Lead when personal data is at risk, and finally to the governance forum for a material exposure.

The privacy commitments apply to the demonstration's handling of personal data; they are stated for the fictional demo and carry no legal effect.

The privacy policy is fictional and carries no legal effect; it exists to show how a real policy is structured, not to bind the provider.

Privacy is reinforced through the awareness program, so the two policies work together rather than as separate documents.

4. Roles and Responsibilities

Role	Illustrative responsibility
Privacy Lead	Owns the policy and the privacy program.
Data Custodian	Applies the technical controls behind each use.
Customer	Acts as controller for the vendor records it submits.
Privacy Reviewer	Reviews processing activities against the notice.
Trust Center Coordinator	Maintains the fictional label on shared copies.

The following RACI is illustrative.

Illustrative RACI for privacy:

Activity	Privacy Lead	Customer	Data Custodian
Describe processing	R	C	I
Provide notice	R	I	I
Apply controls	C	I	R
Handle requests	R	C	I
Review retention	R	I	C

5. Policy Requirements and Controls

PTT-POL-018-C01. Collect the minimum necessary

Only the personal data needed for the described use is collected, so the demonstration does not accumulate data it has no purpose for. Minimal collection reduces both risk and noise. A field is checked for necessity before it is added.

PTT-POL-018-C02. State the purpose

Each use of personal data is tied to a stated purpose, so data is not repurposed silently. A use without a stated purpose is not permitted. The purpose is recorded before collection.

PTT-POL-018-C03. Limit retention

Personal data is kept only for the illustrated retention period, so data does not outlive its purpose. Expired data is deleted per the retention schedule. The deletion date is set and enforced.

PTT-POL-018-C04. Provide individual choices

Access, correction, and deletion requests are supported in the demo, so individuals can act on their data. Requests are routed and answered on a defined cadence. The choice is recorded and honored.

PTT-POL-018-C05. Secure the data

Personal data is protected by the encryption and access controls in this library, so privacy rests on the same controls as security. The data is protected in transit and at rest.

PTT-POL-018-C06. Limit sharing

Personal data is shared only as described and never sold, so data does not leave the boundary through an undisclosed channel. A share is logged with its purpose.

PTT-POL-018-C07. Be transparent

The notice describes collection, use, and sharing in plain language, so a reader can understand the model without legal expertise. The handling is described openly, so there are no surprises.

PTT-POL-018-C08. Honor customer control

Customers remain the controller for the vendor records they submit, so Paper Tiger does not independently repurpose that data. The customer controls its data, and the provider follows.

PTT-POL-018-C09. Document legal bases

Each processing activity has an illustrative legal basis recorded, so the purpose and justification are paired. Each activity records its basis.

PTT-POL-018-C10. Review processing

Processing activities are reviewed against the notice on a cadence, so drift between the notice and reality is caught. The review is dated and a gap is remediated.

PTT-POL-018-C11. Conduct privacy impact review

New processing that involves personal data receives a lightweight privacy review before launch, so privacy is considered at design rather than after deployment. A high-risk activity gets a privacy impact review.

PTT-POL-018-C12. Honor data portability

Individuals can obtain their data in a usable format in the demo, so the choice model includes access as well as deletion. A subject can take their data, so they are not locked in.

PTT-POL-018-C13. Train on privacy

Personnel who handle personal data receive privacy training so the notice is reflected in actual behavior, not just documentation. Handlers are trained, so the rules are understood, not just written.

PTT-POL-018-C14. Document data flows

Personal data flows are documented so the privacy program knows where personal data travels and who touches it. The flows are mapped, so a question can be answered from the map.

PTT-POL-018-C15. Honor opt-out where offered

Where an opt-out is offered, it is honored in the demo, so a choice is not a decoration.

PTT-POL-018-C16. Review third-party privacy

The privacy posture of subprocessors is reviewed, so personal data does not flow to a party with weak privacy. A third party's privacy is reviewed before sharing.

PTT-POL-018-C17. Obtain and record consent where required

Where a purpose relies on consent, the consent is obtained, recorded, and revocable, so the individual retains control over the processing they agreed to. Consent is obtained and recorded, so it can be shown later.

PTT-POL-018-C18. Publish a privacy notice

The demonstration's handling is described in a notice, so individuals can see what happens to their data in the fiction. The notice is published, so individuals can read the handling.

PTT-POL-018-C19. Handle data subject complaints

A complaint is logged and routed to the privacy owner, so a concern is addressed rather than dropped.

PTT-POL-018-C20. State the lawful basis per activity

Each processing activity records the basis it relies on in the fiction, so the demonstration shows the shape of a lawful-basis analysis. Each activity states its basis in the fiction.

PTT-POL-018-C21. Document international transfers

A transfer outside the stated geography is recorded, so the controller can see the movement and its basis.

PTT-POL-018-C22. Maintain a record of processing activities

The provider keeps a current record of its processing, so a question about any activity can be answered from the record. The record is current and its owner is named.

PTT-POL-018-C23. Provide a data subject access workflow

A request to see or correct data follows a defined route through the controller, so the individual's rights are honored consistently. An access request follows a defined route.

PTT-POL-018-C24. Define breach notification to the controller

The provider commits to notify the controller when personal data is compromised, so the controller can meet its own obligations. The controller is notified on a defined basis.

6. Operating Procedures

Describe the processing.

The Privacy Lead documents each use and its illustrative legal basis.

Collect with notice.

Individuals are shown the notice before their data is collected.

Apply controls.

The custodian applies encryption and access limits to personal data.

Handle requests.

Access, correction, and deletion requests are routed and answered.

Review retention.

Data past its retention period is deleted.

Refresh the notice.

The notice is updated when a use changes.

Review processing.

Processing activities are rechecked against the notice.

Run a privacy review.

A new processing activity is reviewed against the notice before launch, and the review is recorded.

Provide a portability export.

A request for data portability is fulfilled in a usable format and logged.

Document a flow.

A personal data flow is recorded with its source, destination, and purpose.

Honor an opt-out.

An opt-out is applied and recorded.

Handle a subject request.

The request is verified, the relevant data is located, the requested action is taken, and the response is logged.

Record a processing activity.

The activity is added to the inventory with its purpose, data types, and retention.

Run a DPIA.

The processing activity is assessed, risks are documented, mitigations are assigned, and the assessment is recorded.

Review the data inventory.

The privacy owner reviews what personal data the demonstration holds, confirms each item has a purpose, and flags anything that does not.

Run a data flow review.

The privacy owner walks the data flow map, confirms each flow has a purpose, and flags any flow that lacks one.

Resolve a privacy complaint.

The privacy owner investigates the complaint, records the outcome, and corrects any handling that was out of line.

Update the processing record.

The privacy owner adds or changes an activity in the record and confirms its purpose and basis are still stated.

Run a privacy-by-design review.

The privacy owner reviews a new processing activity before launch and records any finding.

Execute an erasure request.

The provider deletes the personal data and confirms the result to the controller.

Review consent records.

The owner checks consent records for expiry and re-obtains any that has lapsed.

Review a transfer.

The privacy owner checks a cross-border transfer and records its basis.

Update the notice.

The owner updates the privacy notice when the handling changes.

7. Frequency and SLAs

Illustrative privacy cadence:

Activity	Frequency (illustrative)
Notice review	Annually and on change
Retention review	Annually
Request handling	As received
Processing review	Semi-annually

8. Exceptions and Lifecycle

An exception permits a temporary processing activity outside the notice when the Privacy Lead documents the reason and updates the notice.

Exceptions are reviewed quarterly, and any processing that stays outside the notice across two cycles is stopped or brought into the notice.

Any processing that stays outside the notice across two cycles is stopped or brought into the notice, because a persistent gap between the notice and practice is a compliance failure, not an edge case.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Privacy notice	The current collection and use description.
Processing inventory	The documented uses and bases.
Notice records	The provided notices.
Request logs	The handled individual requests.
Retention records	The applied retention and deletion.
Privacy review records	The pre-launch assessments.
Portability exports	The fulfilled export requests.
Subject request log	The received and fulfilled requests.
Record of processing activities	The maintained list of processing, purpose, and basis.
Complaint log	The recorded complaints and their outcomes.
Consent records	The recorded consents and their scope.
Erasure log	The executed erasure requests.
Privacy-by-design reviews	The dated reviews of new processing.
Data protection records	The documented safeguards.

10. Oversight and Metrics

- Notice currency: reviewed within the cadence (illustrative).
- Request handling: answered within the illustrative window.
- Retention compliance: no personal data past its period.
- Processing drift: zero unlisted uses.
- Privacy review: 100 percent of new processing reviewed before launch.
- Request fulfillment time: the median time to complete a subject request within the stated window.
- Inventory completeness: the share of known processing activities recorded in the inventory.
- Percentage of processing activities with a stated basis.
- Complaints resolved within the committed window.
- Percentage of activities with a stated basis.
- Complaints resolved within the window.
- Erasure requests completed on time.
- Consent records reviewed for expiry.
- New processing reviewed before launch.
- Safeguard gaps found in review.

11. Appendix

Illustrative data uses:

Use	Purpose (illustrative)
Service delivery	Operate the vendor-screening platform

Support	Respond to requests and troubleshoot
Security	Detect and prevent misuse
Legal	Comply with valid legal process

12. Related Policy Dependencies

- Data Processing Addendum (the processor terms behind this notice)
- Data Classification and Handling Policy (governs how personal data is handled)
- Records Retention and Deletion Policy (governs retention)
- Subprocessor List (discloses who processes the data)
- Security Awareness and Training Policy (delivers the privacy training)

13. Review Cadence

The Privacy Lead reviews this policy at least annually, after a change to the illustrated processing, and after a significant simulated privacy event.

Revision History

Version	Date	Change summary	Author
1.0	September 28, 2026	Original enterprise-depth fictional demo policy for controlled trust-center testing.	Paper Tiger Technologies

Document Control

Field	Value
Document ID	PTT-POL-018
Document Owner	Privacy Lead
Status	Fictional demo artifact
Effective Date (illustrative)	September 28, 2026
Review Cadence	At least annually and after material fictional changes
Classification	Internal Demo
Approval	Illustrative governance approval only; no real adoption represented