

PAPER TIGER TECHNOLOGIES

Subprocessor List

1. Purpose

The purpose of this Subprocessor List is to disclose, for the fictional PaperTiger service, the third parties that would help deliver the illustrated platform. It also states how those parties are reviewed and how customers are notified of changes.

Transparency about subprocessors is a core trust expectation: a customer should not discover after the fact that a third party was touching their data. This list is the standing disclosure that supports that expectation, and it pairs each entry with the purpose and data involved.

This list is fictional and illustrative. Every provider name, location, and date is synthetic; no real provider is represented.

The subprocessor list is a trust artifact customers read closely, so the policy keeps it accurate, current, and backed by real diligence rather than a static page.

The list is only as trustworthy as the diligence behind it, so the policy covers residency, exit, and change, the parts a customer's review actually probes.

The subprocessor list exists so the controller can see who touches its data, and the policy makes the list a maintained record with approvals rather than a static name sheet.

The list exists so the controller can see the full chain of who touches its data, and the policy makes that chain visible, current, and approved rather than implied.

2. Definitions

Term	Definition (illustrative)
Subprocessor	A third party engaged to host, support, or process data for the illustrated service.
Data category	The type of data a subprocessor handles.
Due diligence	The review performed before a subprocessor is engaged.
Change notification	The notice to customers before a material list change.
Re-review	The periodic reassessment of an existing subprocessor.
Offboarding	The removal of a subprocessor and confirmation of data disposition.

Register	This list of active subprocessors with purpose and data.
Location (illustrative)	A synthetic region label used to indicate data locality.
Change history	The recorded changes to the register.
Concentration risk	The dependence on a single subprocessor.
Trust center	The customer-facing location where the list is published.
Disclosure	The publication of the current subprocessor list to customers so they can review who handles their data.
Data residency	The geographic location where a subprocessor stores or processes customer data.
Exit plan	The prepared way to move off a subprocessor if the relationship ends or fails.
Flow-down	The passing of obligations from the provider to its subprocessors.
Onboarding	The process of bringing a subprocessor under the required terms.
Fourth-party risk	Risk from a subprocessor's own suppliers.
Vendor tiering	The grouping of subprocessors by criticality.
Onboarding checklist	The standard steps to bring a subprocessor under terms.
Vendor management	The oversight of third-party relationships.
Security assessment	The review of a vendor's security posture.
Data processor	A party that processes data on behalf of the provider.
Concentration review	The check of dependence on a single subprocessor.
Transfer path	The route data takes between the provider and a subprocessor.
Subprocessor change	Any addition, removal, or replacement of a listed party.
Subprocessor inventory	The maintained list of every downstream party and its role.
Engagement	The start of a subprocessor's work under the required terms.

3. Scope and Boundaries

This list applies to fictional subprocessors engaged to host, support, or otherwise process data for the illustrated service. It covers infrastructure, tooling, and support providers.

It applies to every third party that could touch customer data or metadata, regardless of whether the relationship is direct or indirect.

Out of scope are real providers and real services. No entry in this list corresponds to a real company.

The scope includes indirect relationships, so a subprocessor that itself uses a subprocessor is still disclosed where it touches customer data.

Escalation for a subprocessor issue follows a fixed chain: a failing assessment goes to the vendor owner, then to the Information Security Lead, and finally to the governance forum when customer data is at risk.

A subprocessor stays on the list only while it is actually used and its assessment is current; a vendor whose engagement has ended is removed rather than left to imply an ongoing relationship.

The list is a snapshot of the demonstration's downstream providers; it is fictional and carries no real subprocessor relationships.

The list is reviewed with the DPA so the two artifacts stay consistent, and any mismatch is corrected before either is published.

The list is a fictional demonstration of a real subprocessor disclosure, not a statement of actual relationships.

A subprocessor stays on the list only while it is actually used and its assessment is current.

4. Roles and Responsibilities

Role	Illustrative responsibility
Vendor Management Lead	Owns the list and the review process.
Procurement Reviewer	Performs due diligence before a subprocessor is engaged.
Privacy Lead	Confirms data-protection terms flow down to each subprocessor.
Trust Center Coordinator	Maintains the fictional label on shared copies.

The following RACI is illustrative.

Illustrative RACI for subprocessor management:

Activity	Vendor Mgmt Lead	Procurement Reviewer	Privacy Lead
Assess a candidate	C	R	C
Sign data terms	C	I	R
Add to the list	R	I	C
Notify customers	R	I	C
Re-review	R	C	I

5. Policy Requirements and Controls

PTT-POL-017-C01. Disclose the current list

Active subprocessors are published in this list, so customers can review who touches their data at any time. A hidden subprocessor undermines the trust this list exists to build. The list is published and its date is visible.

PTT-POL-017-C02. Review before engagement

Each subprocessor is assessed before it handles demo data, so a party with weak practices is caught before it is onboarded. The assessment covers security and confidentiality. The assessment is dated and its outcome recorded.

PTT-POL-017-C03. Flow down data terms

Each subprocessor is bound to illustrative data-protection terms, so the protection obligations do not stop at the organizational edge. The terms are recorded. The provider's obligations flow down to the subprocessor.

PTT-POL-017-C04. Notify of changes

Customers are notified before a material addition or change, so they have a chance to object rather than discover a change after it happened. The change notice is dated and its recipient recorded.

PTT-POL-017-C05. Re-review on a cadence

Subprocessors are re-reviewed at least annually, so a party that was sound at onboarding does not silently degrade. The re-review is dated and a stale entry is removed.

PTT-POL-017-C06. Record the data involved

The list states the purpose and data categories for each party, so a customer can assess exposure without asking. The data record is checked for completeness.

PTT-POL-017-C07. Keep names fictional

No real provider is named or implied in this demonstration, preserving the non-production boundary. The names are fictional, so no real vendor is implied.

PTT-POL-017-C08. Offboard cleanly

A retired subprocessor has its access removed and data disposition confirmed, so no dormant access path remains. The offboard requires a return-or-delete confirmation.

PTT-POL-017-C09. Maintain a change history

The register records its own change history so a customer can see when and how the list changed over time, supporting audit and objection. The history records each change, so the list is auditable.

PTT-POL-017-C10. Assess concentration

The vendor management lead assesses concentration risk so the service does not silently become dependent on a single subprocessor. The concentration check runs on a schedule.

PTT-POL-017-C11. Publish in the trust center

The list is published in the trust center where customers can find it, rather than held in an internal document. The list appears in the trust center for customer review.

PTT-POL-017-C12. Document subprocessor responsibilities

Each subprocessor's responsibilities are documented, so the boundary of what they do and the data they touch is clear. Each subprocessor's responsibility is documented.

PTT-POL-017-C13. Review subprocessor security

The subprocessor's security posture is reviewed as part of due diligence, so a weak third party is caught before onboarding. The security of each subprocessor is reviewed.

PTT-POL-017-C14. Publish notification timing

The timing of change notifications is published, so customers know how much notice they will receive. The timing of change notification is published.

PTT-POL-017-C15. Record subprocessor data residency

The location where each subprocessor handles data is recorded, because customers care where their data sits and the disclosure must be accurate. Where the data resides is recorded.

PTT-POL-017-C16. Maintain an exit plan per subprocessor

Each subprocessor has a prepared exit path, so a failure or termination does not leave the platform unable to move the processing elsewhere. Each subprocessor has an exit plan.

PTT-POL-017-C17. Classify each subprocessor by data exposure

Each subprocessor is categorized by whether it can touch customer data, so the depth of review matches the level of exposure. Exposure is classified, so review depth matches risk.

PTT-POL-017-C18. Confirm location and transfer paths

The provider records where each subprocessor operates and where data would flow, so the controller can assess its own transfer obligations. Location and transfer paths are confirmed.

PTT-POL-017-C19. Track the approval trail

Each subprocessor entry keeps its approval date and approver, so the list is a record of decisions rather than an unverifiable inventory. Each entry records its approver and date.

PTT-POL-017-C20. Include the subprocessor's role

Each entry states what the subprocessor does for the service, so a name is not left to be interpreted without context. Each entry states what the subprocessor does.

PTT-POL-017-C21. State the subprocessor's processing purpose

Each entry records why the subprocessor processes data, so the purpose limitation can be checked against the actual engagement. The purpose is stated, so purpose limitation can be checked.

6. Operating Procedures

Assess the candidate.

The procurement reviewer evaluates the subprocessor's security and confidentiality before engagement.

Sign the data terms.

Illustrative data-protection terms are applied and recorded.

Add to the list.

The subprocessor is published with purpose and data categories.

Notify customers.

A notice is sent before the subprocessor begins handling data.

Re-review annually.

The vendor management lead refreshes the assessment on schedule.

Offboard when retired.

Access is removed and data disposition is confirmed.

Record the change.

Every addition, change, and removal is recorded in the register history.

Record the change history.

Every addition, change, and removal is recorded with the date and rationale.

Assess concentration.

The lead reviews whether any single subprocessor has become critical and records the finding.

Document responsibilities.

A subprocessor's scope is documented at engagement.

Publish notification timing.

The notice window is published in the trust center.

Onboard a subprocessor.

The candidate is assessed, contracted, added to the list, and the customer notification is prepared.

Review a subprocessor.

The party is re-assessed against the current standard, and the outcome updates the list and any findings.

Exercise a subprocessor exit.

The exit plan is walked through, data is moved or deleted as required, and the exercise is recorded.

Re-verify the list.

The vendor owner compares the published list to the actual vendors, removes any that are no longer used, and adds any that were missed.

Publish an update.

When the list changes, the provider republishes it and records the date, so customers always see the current version.

Assess a new subprocessor.

The vendor owner drafts the assessment, the Information Security Lead confirms the controls, and the controller is notified before work begins.

Offboard a subprocessor.

The vendor owner confirms return or deletion, records the date, and updates the list.

Conduct due diligence.

The vendor owner reviews the subprocessor's controls and records the assessment.

Update the trust center.

When the list changes, the provider republishes it and records the date.

Review concentration.

The owner checks dependence on a single subprocessor and records any exposure.

Record data residency.

The vendor owner records where each subprocessor's data sits and updates the list.

Maintain an exit plan.

The vendor owner keeps a documented path to offboard each subprocessor cleanly.

Confirm location and transfer paths.

The vendor owner records where each subprocessor operates and where data would flow.

7. Frequency and SLAs

Illustrative subprocessor cadence:

Activity	Frequency (illustrative)
Due diligence	Before engagement
Re-review	Annually
Change notification	Before material change
List review	Quarterly

8. Exceptions and Lifecycle

An exception permits an expedited onboarding for a subprocessor when the Vendor Management Lead documents the urgency and completes the full review shortly after.

Exceptions are reviewed quarterly, and a subprocessor that stays in expedited status across two cycles is reviewed for removal.

A subprocessor that stays in expedited status across two cycles is reviewed for removal, because expedited onboarding that never completes is a standing gap in due diligence.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Current subprocessor list	The active register.

Due-diligence records	The pre-engagement assessments.
Data-term acknowledgments	The flowed-down terms.
Change notifications	The notices to customers.
Re-review records	The periodic reassessments.
Change history	The dated list changes.
Concentration assessment	The dependence review.
Assessment records	The due-diligence review of each subprocessor.
Published list	The current subprocessor list with services and locations.
Subprocessor assessments	The completed reviews for each listed party.
Vendor tier assignments	The recorded criticality tier per subprocessor.
Offboarding confirmations	The return-or-delete confirmations at offboarding.
Vendor register	The maintained list of all vendors.
Assessment reports	The completed security assessments.

10. Oversight and Metrics

- Disclosure completeness: 100 percent of active subprocessors listed (illustrative).
- Re-review completion: 100 percent of due reviews completed.
- Change notification: sent before every material change.
- Unreviewed onboarding: zero subprocessors without a completed assessment.
- Concentration: no single subprocessor beyond the illustrative criticality threshold.
- List accuracy: the share of listed subprocessors matching current engagements.
- Notification timeliness: customer notifications sent within the defined window.
- Percentage of subprocessors with a current assessment.
- Time from subprocessor decision to controller notice.
- Time from decision to controller notice.
- Subprocessors with a fourth-party assessment.
- Time from selection to contract execution.
- Vendors with a current assessment.
- Assessment findings remediated on time.

11. Appendix

Fictional subprocessors (all names and details illustrative):

Subprocessor (fictional)	Purpose	Data categories (illustrative)	Location (illustrative)	Last reviewed (illustrative)
Northpoint Cloud Hosting	Cloud infrastructure and storage	Customer and account data	Region A	2026-06
Signalpath	Data enrichment	Vendor records	Region B	2026-06

Analytics	and scoring support			
Cascade Communications	Transactional email and notifications	Account and contact data	Region A	2026-05
Mereserve Payments	Billing and payment processing	Billing data	Region A	2026-05
Brightline Support	Support ticketing	Support requests	Region B	2026-04
Vantagepoint CRM	Account management	Account and contact data	Region A	2026-04
Atlas Identity	Identity and single sign-on	Authentication events	Region A	2026-03
Redwood Security Labs	Security testing and assessment	None (no customer data)	Remote	2026-03

12. Related Policy Dependencies

- Data Processing Addendum (the terms that flow down to these parties)
- Risk Management Policy (treats third-party risk)
- Privacy Policy (governs personal data sharing)
- Information Request Policy Statement (governs requests involving these parties)

13. Review Cadence

The Vendor Management Lead reviews this list at least annually, after a subprocessor change, and after a significant simulated third-party 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-017
Document Owner	Vendor Management 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