

PrivateStack Data Flow Overview

Version 1.2 - Last reviewed: 2026-07-27

The hosted and Enterprise BYOC request paths are different. This overview states the current boundary for each tier without extending Enterprise claims to hosted workspaces.

Hosted request path

- A user sends a request from an isolated PrivateStack workspace. Policy checks run and request activity is recorded in the tenant audit trail.
- A disclosed US-based inference subprocessor processes the prompt in memory under contractual zero-retention terms, returns the response, and does not use it for training.
- Tenant audit records are retained according to the configured retention policy and can be exported for review.

Enterprise BYOC request path

- PrivateStack deploys the workspace and inference path inside the customer's own AWS account. AWS is the only cloud currently supported for BYOC.
- Prompts, outputs, logs, and knowledge bases remain inside the customer-controlled VPC for the verified Enterprise BYOC configuration.

Controls on every tier

- Connections use TLS. Tenant data stores and backups are encrypted at rest. Request activity is logged and exportable.

Full detail and the subprocessor table are available at privatestackhub.com/trust. Subprocessor names are available under NDA or in an executed DPA. Questions: security@privatestackhub.com.

Tier boundary: hosted privacy is contractual; Enterprise BYOC places the verified inference path inside the customer's AWS VPC.