

PII Data Flows — PortalPilot

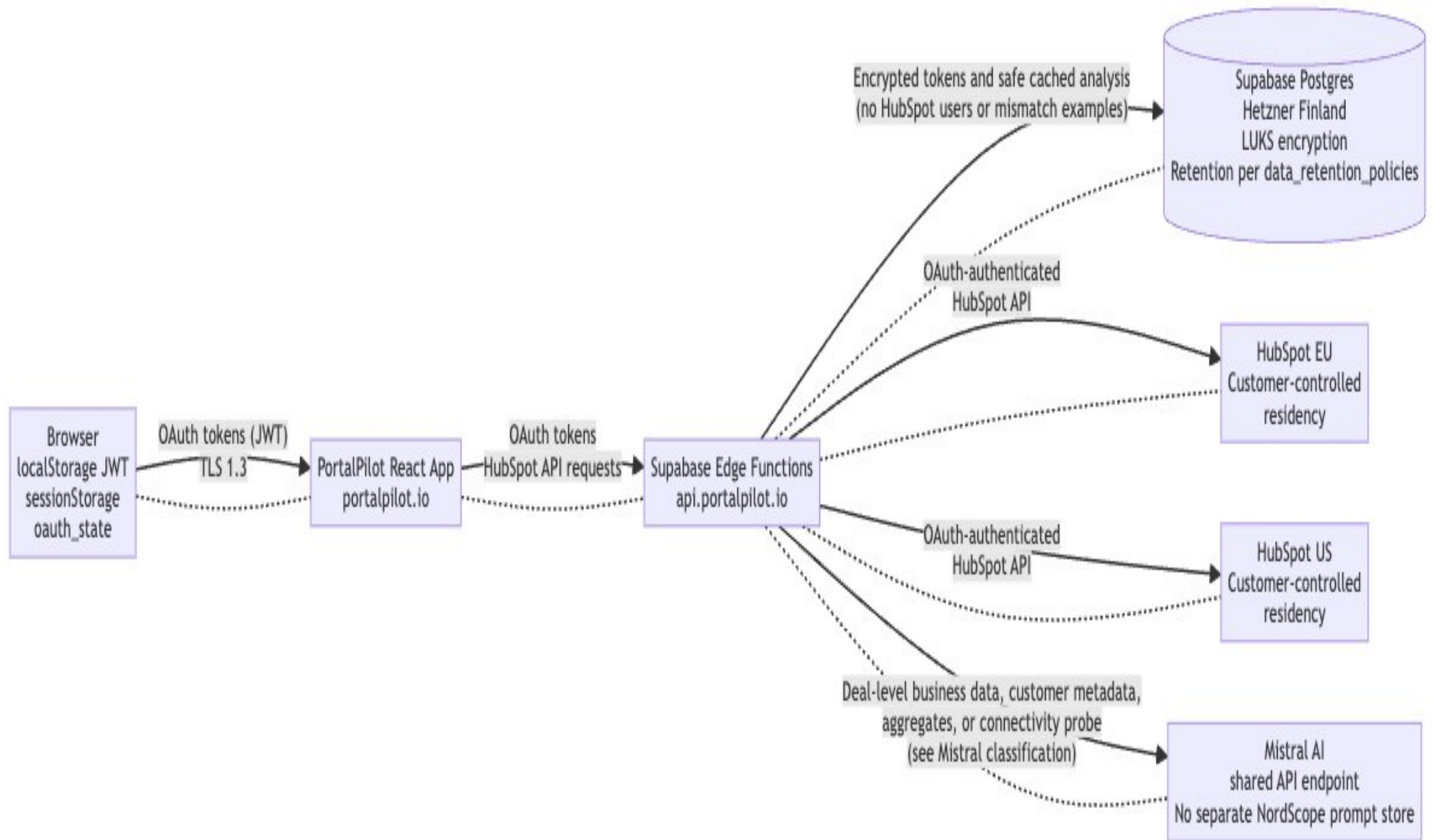
Three diagrams covering customer-facing data flows, operational flows, and third-party I/O. Pictures complement the matrix in the [PII inventory](/trust/pii-inventory.pdf).

****Internal counterpart with NDA-only detail****: available under NDA on request.

****Data controller****: NordScope (toiminimi/sole trader), Y-tunnus 3148476-5. Privacy contact: privacy@portalpilot.io.

Legend

Diagram 1: Customer data plane

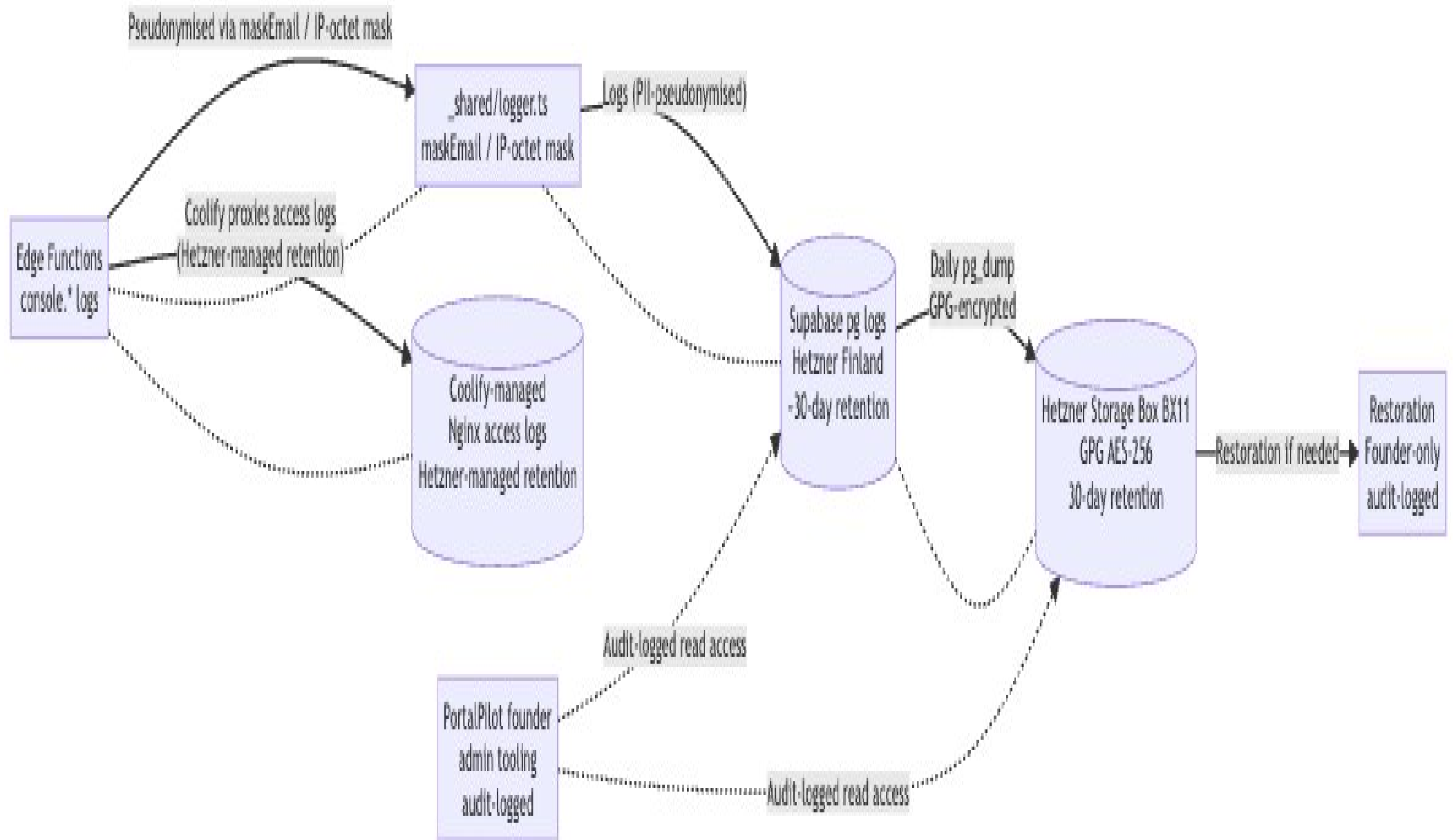


****HubSpot residency note****: residency depends on the customer's HubSpot portal setting (EU or US). PortalPilot does NOT relocate data — the customer's choice flows through.

****Mistral payload note****: 20 edge functions import a shared Mistral helper. See the [PII inventory](/trust/pii-inventory.pdf) for the exact helper and payload class for each function.

****Analysis storage note****: the immediate response may contain detailed findings. Persistent `cached\_analysis` stores only the safe projection, which omits HubSpot users and mismatch example values. Analysis history stores scores and counts.

Diagram 2: Operational plane

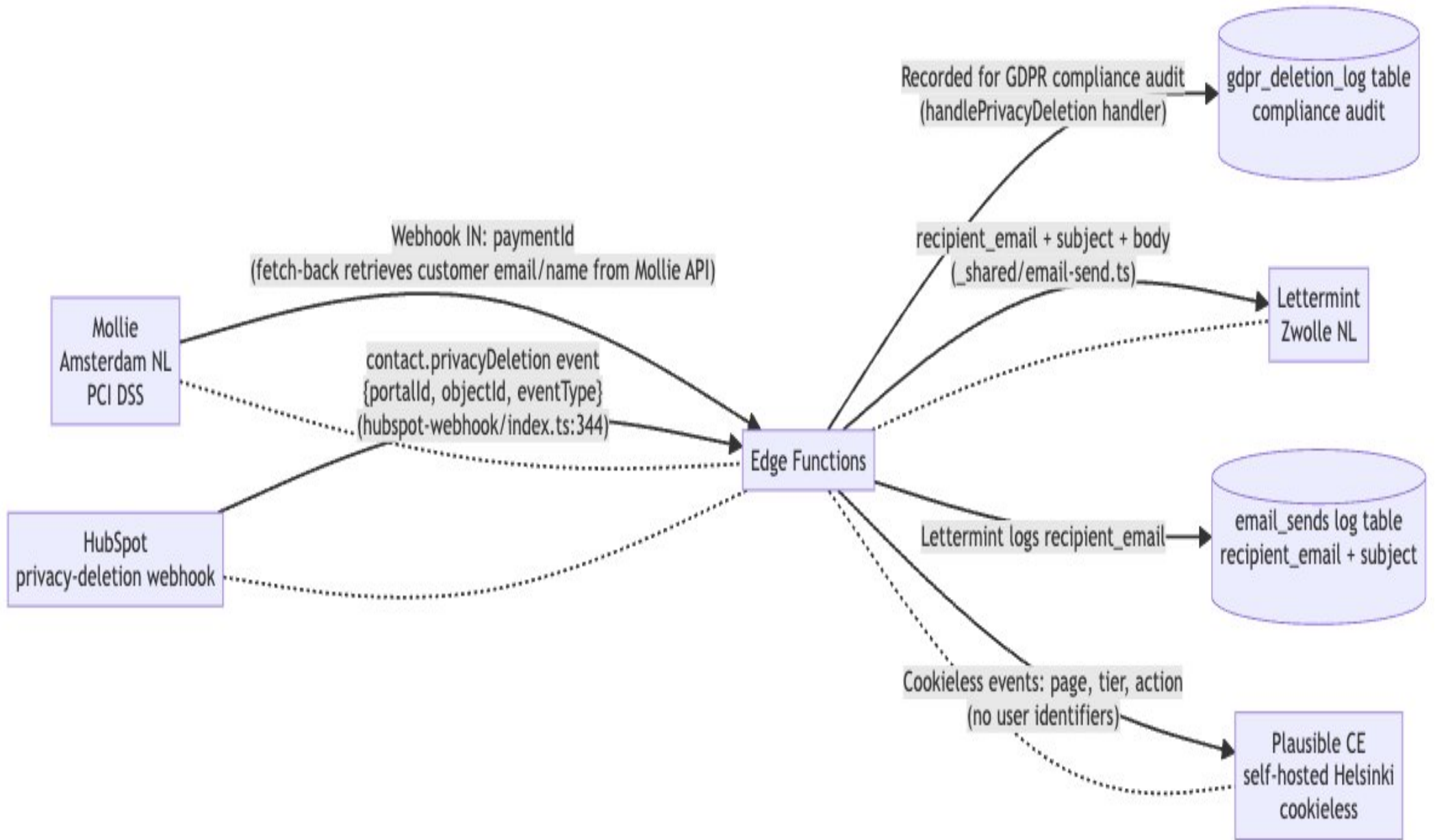


****Admin-access note**** (public version): PortalPilot founder access via authenticated admin tooling, audit-logged. The full operational mechanism is documented under NDA on request.

****Hetzner-managed log note****: Coolify-managed Nginx access logs are NOT under direct NordScope control of retention. Mitigation: upstream Coolify configuration plus the documented operational-discipline escalation procedure (NDA counterpart) for any PII leak found in those logs.

****Footnote — PWA service worker cache****: PortalPilot's PWA service worker caches ONLY static assets (`js`, `css`, `ico`, `png`, `svg`, `woff2`) per `vite.config.ts` `globPatterns` (line 112). NO HTML, JSON, or API responses are cached. Browser-side PII (auth JWT) is in `localStorage`, not in the service-worker cache.

Diagram 3: Third-party I/O plane



****Plausible event scope****: 15 non-test `trackEvent(...)` calls across 9 source files, checked against the source inventory in CI. Props are limited to `{page, tier, action, method, accountType}` and contain no user identifiers. The earlier count of 16 included the function declaration, which does not send an event. Plausible is cookieless and self-hosted at `analytics.portalpilot.io`.

****Lettermint logging****: `supabase/functions/_shared/email-send.ts` writes `recipient_email`, `subject`, `email_type`, `user_id`, `status`, `sent_at` to the `email_sends` logging table on send. The `EmailLog` node in Diagram 3 represents this table — it stores delivery metadata + recipient address, not message body. See the [PII inventory](/trust/pii-inventory.pdf) row 22 for retention.

****HubSpot privacy-deletion handler****: `handlePrivacyDeletion` resolves the external HubSpot portal ID to PortalPilot's internal portal UUID and deletes that portal's cached analysis before it records success in `gdpr_deletion_log`. Lookup or deletion failure is retryable. An unknown portal is recorded as no data held.

Footnote: Agent-plane data (NOT customer PII)

Claude Code session memory, the agent memory subsystem, and the agent-side hook audit log are operational metadata internal to the development process. They are NOT customer PII.

These flows fall under the supplier-relationship controls (ISO 27001 Annex A.5.19–A.5.23) — see the [ISO 27001 Annex A control register](/compliance/iso27001-annex-a-register.html).

Last review

Field	Value
Document	PII data flows
Owner	Founder (NordScope)
Cadence	Annual + per-release for new data flows
Last reviewed	2026-09-06
Next review due	2026-Q4