PII Inventory — PortalPilot

PortalPilot's complete inventory of personal data (PII) processed by the application, organised by surface: application data plane, audit + operational data, browser-side state, third-party I/O, application output, and server-side operational surfaces.

Internal counterpart with NDA-only detail: founder admin-access mechanism and lawful-intercept specifics, available under NDA on request.

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

Inventory matrix

Application data plane (10 categories)

#	Field	Source	Where stored	Encryption at rest	Encryption in transit	Retention	Data minimisation rationale	Lawful basis (Art 6)	Visibility to customer	Sub-processors with access	GDPR rights enforcement (Art 15/17/20)	Pseudonymisation status
1	Account email	User signup via `Auth.tsx` ! Supabase Auth	`auth.users.email`	Hetzner full-disk encryption (LUKS)	TLS 1.3 (Coolify reverse proxy)	Until account deletion + 30-day grace per Privacy §5	Required for login + transactional email	Art 6(1)(b) Contract	Yes — visible on the consumer dashboard (`Dashboard.tsx`); deletion via `DeleteAccountDialog.tsx`	Hetzner (database at-rest), Lettermint (when sending email)	Art 15: full export on request via privacy@portalpilot.io; Art 17: account-delete cascade; Art 20: SQL export available	Pseudonymised in logs via `maskEmail` (`_shared/logger.ts:29`)
2	Account display name	User signup or profile edit	`auth.users.raw_user_meta_data` (canonical Supabase schema)	LUKS	TLS 1.3	Until account deletion + 30-day grace	Required for personalised UI + email salutations	Art 6(1)(b) Contract	Yes — editable from the consumer dashboard	Hetzner	Art 15/17/20 same as Account email	Not pseudonymised in logs (display names rarely appear in `console.*`; sample audit per S10)
3	`portal_id` (HubSpot portal identifier)	HubSpot OAuth callback	`portals.portal_id`, foreign-keyed across `portal_credentials`, `hubspot_write_operations`, `partner_client_portals`, `data_retention_policies`, `rate_limit_buckets`, `idempotency_cache`, `analyses`	LUKS	TLS 1.3	Until customer disconnects portal or deletes account	Required to identify the customer's HubSpot tenant	Art 6(1)(b) Contract	Yes — visible in URL (`/portal/:id`) and on dashboard	Hetzner; HubSpot (the customer's own platform)	Art 15/17/20 via account deletion or portal disconnect	Quasi-PII per GDPR Recital 30; not masked in logs (treated as non-sensitive identifier)
4	`portal_name`	HubSpot Companies API on first connect	`portals.portal_name`	LUKS	TLS 1.3	Same as portal_id	Required for portal identification in UI	Art 6(1)(b) Contract	Yes — visible on dashboard + portal switcher	Hetzner	Art 15/17/20 via portal disconnect or account deletion	Not pseudonymised
5	OAuth `access_token`	HubSpot OAuth grant	`portal_credentials.access_to	**AES-256-GCM	TLS 1.3	Until token	Required	Art	No — not exposed to	Hetzner	Art 17: deleted	Stored encrypted;

#	Field	Source	Where stored	Encryption at rest	Encryption in transit	Retention	Data minimisation rationale	Lawful basis (Art 6)	Visibility to customer	Sub-processors with access	GDPR rights enforcement (Art 15/17/20)	Pseudonymisation status
	(HubSpot)		ken`	** (PBKDF2 100k iterations, random 16-byte salt per operation; see `_shared/crypto.ts:87`) on top of LUKS		rotation, portal disconnect, or account deletion	to call HubSpot APIs on the customer's behalf	6(1)(b) Contract	customer (security boundary)	(encrypted ciphertext only); HubSpot (when used to call HubSpot APIs)	on portal disconnect or account deletion	never logged in plaintext
6	OAuth `refresh_token` (HubSpot)	HubSpot OAuth grant	`portal_credentials.refresh_token`	AES-256-GCM same as access_token	TLS 1.3	Same as access_token	Required to refresh expired access tokens	Art 6(1)(b) Contract	No	Hetzner (ciphertext only); HubSpot	Art 17 same as access_token	Stored encrypted; never logged in plaintext
7	`token_expires_at`, `last_refresh_at`	OAuth grant + refresh events	`portal_credentials.token_expires_at`, `last_refresh_at`	LUKS	TLS 1.3	Same as access_token	Required for token-rotation logic	Art 6(1)(b) Contract	No (operational metadata)	Hetzner	Art 17 same as access_token	Not PII alone; correlatable with portal_id
8	HubSpot record samples (transient)	HubSpot API responses during analysis	**Not persisted** — held in memory in the edge function for the duration of the request only	N/A (in-memory only)	TLS 1.3 inbound from HubSpot, TLS 1.3 outbound to Mistral when AI analysis is requested	None — record samples are never written to disk	Required to compute analysis output	Art 6(1)(b) Contract (instructed processing)	Indirect — analysis output references aggregated findings, not record-by-record samples	Mistral (when an AI-bearing function is invoked; see Mistral classification below)	Art 15/17/20 not applicable (not persisted)	N/A — transient
9	Team-membership records	Team-member invite flow via the consumer dashboard (`Dashboard.tsx`) and `AcceptInvite.tsx`	`partner_client_portals` (portal_id, user_id, role)	LUKS	TLS 1.3	Until membership revoked or account deleted	Required for multi-user portal access (Solutions Partner use case)	Art 6(1)(b) Contract	Yes — visible to all team members on the portal	Hetzner	Art 15/17/20 cascade with account deletion; team-member can self-leave	RLS-protected per `partner_client_portals` policies
10	`data_retention_policies` rows	Policy configuration via `PolicyConfigurationView`	`data_retention_policies` (portal_id, data_type, retention_period_days)	LUKS	TLS 1.3	Until portal disconnect or account deletion	Customer policy choice (configuration; arguably non-PII)	Art 6(1)(b) Contract	Yes — visible + editable in policy UI	Hetzner	Art 17 cascade with portal disconnect	Configuration data; not PII alone

Audit + operational data (4 categories)

#	Field	Source	Where stored	Encryption at rest	Encryption in transit	Retention	Data minimisation rationale	Lawful basis (Art 6)	Visibility to customer	Sub-processors with access	GDPR rights enforcement (Art 15/17/20)	Pseudonymisation status
11	`hubspot_write_operations.before_value` JSONB	Edge function performing a HubSpot property write	`hubspot_write_operations.before_value`	LUKS	TLS 1.3	**90 days** per migration `20260129_write_operations_audit.sql` (cron-enforced via `cleanup_old_write_operations`)	Required for write-operation audit trail (security + change-history)	Art 6(1)(f) Legitimate interest in audit trail	Indirect — surfaces in audit-log views	Hetzner	Art 17 cascade with portal disconnect (90-day rolling retention); Art 15 export available on request	**May contain PII**: contact `email`/`firstname`/`lastname`/`phone`/`address`; company name/address; deal contact references. See "Audit-log JSONB PII coverage" section below for the full enumeration.
12	`hubspot_write_operations.after_value` JSONB	Same as #11	`hubspot_write_operations.after_value`	LUKS	TLS 1.3	90 days same as #11	Required for change-delta audit	Art 6(1)(f)	Indirect	Hetzner	Same as #11	Same as #11
13	`hubspot_write_operations.user_id`, `portal_id` columns	Edge function metadata	`hubspot_write_operations.user_id`, `.portal_id`	LUKS	TLS 1.3	90 days	Required to attribute writes to a user + portal	Art 6(1)(f)	Indirect	Hetzner	Art 17 cascade	`user_id` is the Supabase auth UUID (not directly identifying); `portal_id` is HubSpot's tenant ID
14	`rate_limit_buckets`, `idempotency_cache` keys	Edge-function rate-limit + idempotency machinery	`rate_limit_buckets.key`, `idempotency_cache.key`	LUKS	TLS 1.3	Short-lived (rate-limit window + idempotency TTL, typically minutes to hours)	Required for abuse prevention + idempotent webhook handling	Art 6(1)(f)	No	Hetzner	Auto-expires; no Art 17 action required	Keys composed from user_id + portal_id (UUIDs); not directly identifying

Browser-side state (3 categories)

#	Field	Source	Where stored	Encryption at rest	Encryption in transit	Retention	Data minimisation rationale	Lawful basis (Art 6)	Visibility to customer	Sub-processors with access	GDPR rights enforcement (Art 15/17/20)	Pseudonymisation status
15	Browser-side auth JWT	Supabase Auth client default	Browser `localStorage` (`sb-<ref>-auth-token`)	Browser-side; depends on user's device disk encryption	TLS 1.3	Until session expiry, logout, or device storage clear	Required for session continuity across page refreshes	Art 6(1)(b) Contract	Yes — user controls their own browser storage	None (client-side only)	User can clear storage; sign-out invalidates server-side; account deletion revokes all sessions	Standard JWT; payload contains user UUID, email, expiry — not transmitted off-device except as `Authorization` header
16	`ImpersonationContext` sessionStorage payload	Founder admin tool (admin-only feature)	Browser `sessionStorage`	Browser-side	TLS 1.3 (when carried in admin requests)	Tab close	Required for support workflows on admin's own device	Art 6(1)(f) Legitimate interest in customer support	No (admin-only feature, not a customer surface)	None	Cleared on tab close	Admin-side only; not visible to customers
17	`auth_return_to`, `hubspot_oauth_state` sessionStorage values	OAuth flow + post-login redirect machinery	Browser `sessionStorage`	Browser-side	TLS 1.3	Brief — cleared after OAuth callback completes	Required for OAuth state-nonce verification + return-to-page routing	Art 6(1)(b) Contract	Yes — user controls own browser	None	Cleared automatically	`auth_return_to` may contain a URL with PII query params (rare); state-nonce is non-PII

Third-party I/O (5 categories)

#	Field	Source	Where stored	Encryption at rest	Encryption in transit	Retention	Data minimisation rationale	Lawful basis (Art 6)	Visibility to customer	Sub-processors with access	GDPR rights enforcement (Art 15/17/20)	Pseudonymisation status
18	Plausible analytics events	`trackEvent(...)` call sites in app code	Self-hosted Plausible CE at `analytics.portalpilot.io` (Hetzner Finland)	LUKS	TLS 1.3	Plausible CE retention default (configurable per Plausible setup)	Required for product analytics + funnel diagnostics	Art 6(1)(f) Legitimate interest in product improvement	Indirect — `/privacy` describes the cookieless analytics policy	Plausible (self-hosted on PortalPilot infrastructure — same provider as DB)	Cookieless; no user identifiers stored. Account deletion has no Plausible-side effect because Plausible never received an identifier in the first place.	**Cookieless under GDPR Recital 30**; props limited to `{page, tier, action, method, accountType}`. Verified 24 `trackEvent(...)` call sites in `src/`; event labels include "Analysis Complete", "Analysis Started", "CTA Click", "Login", "Signup", "Portal Connected", "Magic Link Sent", "Onboarding Type Selected"

#	Field	Source	Where stored	Encryption at rest	Encryption in transit	Retention	Data minimisation rationale	Lawful basis (Art 6)	Visibility to customer	Sub-processors with access	GDPR rights enforcement (Art 15/17/20)	Pseudonymisation status
19	Mistral AI prompt content	Edge functions invoking `chatCompletion`	**Not persisted by NordScope**; transmitted to Mistral AI (Paris, France Ø	TLS 1.3 in transit; Mistral DPA defines their at-rest handling	TLS 1.3	None NordScope-side; Mistral DPA confirms zero training-on-customer-data and EU residency	Required for AI-driven analysis features (per-function classification below)	Art 6(1)(b) Contract (where AI analysis is part of the requested feature)	Indirect — analysis output is shown; the prompt itself is not	Mistral AI (Paris, EU)	Account deletion stops further prompts; past prompts are not stored by NordScope. Mistral DPA defines their handling.	**Per-function classification table below** distinguishes PII-bearing / pseudonymised-aggregates / config-only
20	Mollie webhook payloads (in)	Mollie webhook on payment events	Edge function `mollie-webhook` processes inline; webhook fetch-back retrieves customer email/name from Mollie API	LUKS (when stored to `payments` table)	TLS 1.3	Per `data_retention_policies.financial_records` policy (180-day default for `analytics_data`; financial_records mapped via the same enforcement function)	Required for payment processing	Art 6(1)(b) Contract	Indirect — order/billing surfaces in account UI	Hetzner; Mollie (as the original source)	Art 15/17 cascade with account deletion; financial-record retention may extend per accounting law	Card details NEVER stored by NordScope (Mollie processes them; PCI-DSS Mollie boundary). Email + name retrieved fresh from Mollie API per request.
21	HubSpot privacy-deletion webhook payload (in)	HubSpot `contact.privacyDeletion` event	Processed inline by `hubspot-webhook/index.ts` (handler at `handlePrivacyDeletion`); recorded to `gdpr_deletion_log` for compliance audit	LUKS	TLS 1.3	`gdpr_deletion_log` retention follows audit-trail policy	Required to honour the customer's HubSpot-side delete request across PortalPilot's analysis logs	Art 6(1)(c) Legal obligation (GDPR Art 17)	Indirect — confirmed via the customer's HubSpot tenant	Hetzner; HubSpot (as the trigger source)	This IS the Art 17 enforcement mechanism for HubSpot-originated deletions	Payload is `{portalId, objectId, eventType}` only — no contact data carried in the payload itself
22	Lettermint transactional email (out)	`_shared/email-send.ts` send + log	Logged to `email_sends` table (`recipient_email`, `subject`, `email_type`, `user_id`, `status`, `sent_at`)	LUKS	TLS 1.3	Per `email_sends` retention policy (operational logging)	Required for delivery troubleshooting + bounce handling	Art 6(1)(b) Contract for transactional emails; Art 6(1)(a) Consent for marketing emails (Privacy §3)	Indirect — surfaces if a delivery issue is reported	Hetzner (database); Lettermint (delivery transit; Lettermint does not retain email content beyond delivery per Privacy §6)	Art 17 cascade with account deletion	`recipient_email` stored in plain text in the log table for delivery audit (acceptable per Privacy §5 retention disclosure)

Application output (2 categories)

#	Field	Source	Where stored	Encryption at rest	Encryption in transit	Retention	Data minimisation rationale	Lawful basis (Art 6)	Visibility to customer	Sub-processors with access	GDPR rights enforcement (Art 15/17/20)	Pseudonymisation status
23	`feedback` table submissions	`FeedbackWidget.tsx` (free-form user input)	`feedback.content` + `user_id`	LUKS	TLS 1.3	Until reviewed + actioned (no automated retention policy currently — operational backlog)	Required to act on user feedback	Art 6(1)(f) Legitimate interest in product improvement	Yes — submitter sees own submission as toast on submit	Hetzner	Art 15: export on request; Art 17: cascade with account deletion	Free-form user content may include any PII the user voluntarily provides
24	`analyses` / `analysis_history` output	Analysis pipeline output	`analysis_history` (per `data_retention_policies` `analytics_data` mapping)	LUKS	TLS 1.3	**180 days default** per migration `20260323212000_insert-default-retention-policies.sql` (configurable per portal)	Required for trend + comparison views	Art 6(1)(b) Contract	Yes — visible in analysis-history UI	Hetzner	Art 17 cascade via portal disconnector account deletion; per-portal retention configurable	**May contain quoted property values from customer data**, including any sensitive identifiers exposed via the analysis (`supabase/functions/analyze-properties/sensitive-data.ts` enumerates the property-name patterns that get flagged in output)

Server-side operational (3 categories)

#	Field	Source	Where stored	Encryption at rest	Encryption in transit	Retention	Data minimisation rationale	Lawful basis (Art 6)	Visibility to customer	Sub-processors with access	GDPR rights enforcement (Art 15/17/20)	Pseudonymisation status
25	Server logs	Edge function `console.*`, Supabase pg logs, Coolify-managed Nginx access logs	Supabase pg logs (DB container, Hetzner Finland); Coolify-managed Nginx access logs (Hetzner-managed retention; **NordScope does not directly control retention for the Nginx access-log path** — see operational-discipline escalation procedure)	LUKS	TLS 1.3	Supabase pg logs: ~30-day operational retention; Nginx access logs: Coolify default	Required for incident response + abuse detection	Art 6(1)(f) Legitimate interest in operational security	No (operational only)	Hetzner; Coolify (managed-runtime layer)	Art 15: log export on request; Art 17: best-effort scrub via Coolify support escalation if PII found	Edge function logs: pseudonymised via `maskEmail` and IP-octet-mask helpers in `_shared/logger.ts`. Sample-audit per S10 verifies coverage.
26	Backup chain	Daily `pg_dump` of `public` +	`/opt/backups/supabase/*` on the application server, then rsynced	**GPG AES-256** on	TLS 1.3 (rsync-over-SSH)	**30 days** rolling	Required for disaster	Art 6(1)(f) Legitimate	No (operational	Hetzner (storage); restore is	Account-deletion does NOT	Backup tarballs are encrypted blobs; not

#	Field	Source	Where stored	Encryption at rest	Encryption in transit	Retention	Data minimisation rationale	Lawful basis (Art 6)	Visibility to customer	Sub-processors with access	GDPR rights enforcement (Art 15/17/20)	Pseudonymisation status
		`auth` schemas	to Hetzner Storage Box BX11 (separate physical machine)	top of LUKS; backup files are encrypted-at-rest with a separate key from the running database			recovery	interest in business continuity	only)	founder-only and audit-logged	immediately remove rows from existing backup tarballs; rows age out within 30 days as backups roll over	searchable without restore; restoration is audit-logged
27	Security incident notifications	`security-incident` edge function	Sent via Lettermint to `privacy@portalpilot.io` (founder-monitored mailbox)	N/A (transient send)	TLS 1.3	Email retention in the founder mailbox (operational; no automated purge)	Required to alert on security events	Art 6(1)(f) Legitimate interest in operational security	No (operational only)	Lettermint (delivery)	N/A (operational notifications, not customer-data records)	Notifications carry incident metadata (event type, timestamp, portal_id) — not record-level PII

Mistral AI per-function PII classification

PortalPilot invokes Mistral AI (`mistral-small-latest`, hosted in Paris, France Ø<ÝëØ<Ý÷) across **19 edge functions
PII payload sent to Mistral per function:

Edge function	LLM call site	Payload classification	Rationale
`account-planning-assistant`	`chatCompletion`	**PII-bearing**	Receives account data (company names + contact details) for account-plan generation
`ai-description-generator`	`chatCompletion`	**PII-bearing**	Receives existing HubSpot property names + sample property values; values may contain customer-identifying content
`ai-naming-suggestions`	`chatCompletion`	Pseudonymised aggregates only	Receives existing property-name patterns for renaming suggestions; no record-level PII
`backend-health-check`	`chatCompletion`	Config-only	"OK" probe payload; no customer data
`churn-prevention-engine`	`chatCompletion`	**PII-bearing**	Receives deal records (company names + contact identifiers) for churn-risk analysis
`competitive-intelligence-ai`	`chatCompletion`	Config-only	Competitor product names from configuration; no customer data
`customer-segmentation-engine`	`chatCompletion`	**PII-bearing**	Receives lifecycle-stage + deal data including company names
`deal-prioritization-engine`	`chatCompletion`	**PII-bearing**	Receives deal records with company + contact context
`deal-risk-analyzer`	`chatCompletion`	**PII-bearing**	Receives deal records + contact info
`generate-executive-summary`	`chatCompletion`	Pseudonymised aggregates only	Receives CRM health metrics + counts; no record-level PII
`generate-remediation-playbook`	`chatCompletion`	Pseudonymised aggregates only	Receives diagnostic findings + counts; no record-level PII
`lead-scoring-optimizer`	`chatCompletion`	**PII-bearing**	Receives contact records (email + name + score features)

Edge function	LLM call site	Payload classification	Rationale
`predictive-data-quality-alerts`	`chatCompletion`	Pseudonymised aggregates only	Receives data-quality findings + counts; no record-level PII
`revenue-forecast-ai`	`chatCompletion`	Pseudonymised aggregates only	Receives pipeline value aggregates; no record-level PII
`revops-advisor`	`chatCompletion`	Pseudonymised aggregates only	Receives aggregated portal stats (counts, percentages, scores); no record-level PII
`sales-forecast-engine`	`chatCompletion`	Pseudonymised aggregates only	Receives pipeline + historical aggregates
`sales-pipeline-optimizer`	`chatCompletion`	Pseudonymised aggregates only	Receives pipeline-stage counts + amount aggregates
`smart-property-suggestions`	`chatCompletion`	**PII-bearing**	Receives existing property names + sample values; values may include customer-identifying content
`win-rate-predictor`	`chatCompletion`	Pseudonymised aggregates only	Receives historical win/loss aggregates

Summary: 8 PII-bearing, 9 pseudonymised-aggregates-only, 2 config-only.

Sub-processor: Mistral AI, Paris, France (EU). DPA reference: see [Data Processing Addendum](/dpa) §4.1.
Trust commitment: Mistral DPA confirms zero training-on-customer-data and EU residency.

Audit-log JSONB PII coverage

The `hubspot_write_operations` table (migration `20260129_write_operations_audit.sql`, **90-day retention** enforced via `cleanup_old_write_operations` cron) captures property change deltas in two JSONB columns:

For HubSpot **contact** properties, these may contain:

For HubSpot **company** properties:

For HubSpot **deal** properties:

Retention: 90 days from operation timestamp, enforced via the `cleanup_old_write_operations` cron job.

Access: RLS-protected by `portal_id`; only the portal owner and team members per `partner_client_portals` RLS policy can read.

Sub-processor exposure: Hetzner (database at-rest only; LUKS); no third-party sub-processor reads `hubspot_write_operations` rows.

Cross-reference consistency

The inventory above is supplementary procurement evidence and does not extend disclosure beyond [Privacy](/privacy), the [Data Processing Addendum](/dpa), and the [Security](/security) page. The three subtables below verify alignment in both directions: every legal-doc category appears here, and every PII-bearing DB table is either represented here or explicitly classified non-PII with reason.

When a drift is found, the legal-doc-wins rule applies: the inventory MUST NOT silently extend coverage beyond what is disclosed in the legal artefacts (which would put NordScope in a position of having undisclosed processing). Discrepancies become triage Issues with labels `triage` + `pii-inventory-discrepancy`, not silent edits.

Subtable 1: Privacy Policy §2 ("Personal data we collect") vs inventory

Privacy §2 category	Status	Inventory row(s)
Account data — email, password (encrypted), full name	' M a t c h e (	rows 1, 2 (account email + display name); password is `auth.users.encrypted_password` (Supabase-managed; bcrypt)
HubSpot portal metadata — portal ID, portal name, property definitions	' M a t c h e (	rows 3, 4 (portal_id + portal_name); property definitions are part of analysis output (row 24)
HubSpot record samples (transient)	' M a t c h e (	row 8 (in-memory only, never persisted)
Lead data — email addresses for newsletter subscribers	' M a t c h e (	covered under row 22 (Lettermint email logging) for marketing emails per Art 6(1)(a) Consent
Usage data — analysis history, property actions, timestamps	' M a t c h e (	row 24 (`analyses` / `analysis_history`) + row 11/12 (`hubspot_write_operations`)
Payment data — Mollie transaction records	' M a t c h e (	row 20 (Mollie webhook payloads + `payments` table); card details NOT stored by NordScope

Subtable 2: Data Processing Addendum Annex I (Personal Data) vs inventory

DPA Annex I category	Status	Inventory row(s)
Account information — email, names, authentication data	' M a t c h e d	rows 1, 2, 15 (browser auth JWT)
HubSpot portal metadata — property names, types, descriptions, usage statistics	' M a t c h e d	rows 3, 4 + analysis output (row 24)
R e c o r d s a m p l e d a t a (t r a n s i e n t , " d 1 , 0 0 0 r e c o r d s p e r o b j e c t t y p e)	' M a t c h e d	row 8
Analysis data — health scores, recommendations, action history (aggregate)	' M a t c h e d	row 24

DPA sub-processors (Annex II §4.1) cross-checked against inventory "Sub-processors with access" column:

DPA sub-processor	Inventory rows referencing	Status
Hetzner Online GmbH (DE/FI hosting)	All rows with at-rest data	' M a t c h e d
Mollie B.V. (NL payments)	row 20	' M a t c h e d
Mistral AI (FR AI processing)	row 19 + Mistral classification table (19 functions)	' M a t c h e d
Lettermint B.V. (NL email)	rows 22, 1 (for transactional email)	' M a t c h e d

Subtable 3: Security page data-handling table vs inventory

Security page disclosure	Status	Inventory row(s)
OAuth tokens encrypted with AES-256-GCM (PBKDF2, 100k iterations, 16-byte salt)	' Matched	rows 5, 6 (with `_shared/crypto.ts:87` citation)
TLS 1.2+ in transit	' Matched (TLS 1.3 across the inventory; 1	every row's "Encryption in transit" column
GPG AES-256 encrypted backups, off-server	' Matched	row 26 (Hetzner Storage Box BX11)
Row-Level Security on every table	' Matched	rows 9, 11-14 mention RLS scope; full RLS coverage is `Security.tsx` policy
90-day audit log retention	' Matched	rows 11, 12, 13 (`hubspot_write_operations`) + Audit-log JSONB section
Account-deletion across 40+ tables	' Matched	rows 1-10 GDPR rights enforcement column ("Art 17 cascade")
HubSpot OAuth 2.0 (no password storage)	' Matched	rows 5, 6 (OAuth tokens only)

Reverse coverage: every PII-bearing DB column is accounted for

The 9 PII-bearing tables (per `scripts/assert-pii-inventory-coverage.mjs`) — `accounts`, `portals`, `portal_credentials`, `hubspot_write_operations`, `partner_client_portals`, `feedback`, `data_retention_policies`, `rate_limit_buckets`, `idempotency_cache` — every column added in any migration is classified by one of:

The CI "Compliance asserts (PII inventory + drift)" step fails the build if any new column is added without one of the three classifications.

Discovery and disclosure policy

Any "&" finding in the subtables above becomes a triage GitHub Issue with labels `triage` + `pii-inventory-discrep

Direction rule: the legal artefacts win for v1 — the inventory cannot extend coverage beyond what is disclosed in those documents. If the inventory finds a processing activity not disclosed in the legal artefacts, the resolution is to update the legal artefacts (in a separate PR) before adding the inventory row, never the other way around.

At time of authoring (2026-04-30), the only outstanding discoveries are spec/plan undercount drifts in [Issue #896](https://github.com/nordscope-fi/portalpilot/issues/896) (Mistral edge-fn count 10!'19; Plausible `trackEvent` 16!'24); both are corrected inline above without changing the legal dis as sole AI sub-processor — is unchanged).

S10 — Pseudonymisation audit (sample of 20 edge functions)

Methodology

Sampled the 20 highest-byte-volume edge functions from `supabase/functions/` (per `du -s` ranking on 2026-04-30). The plan specified "highest-volume by deploy frequency"; PortalPilot is self-hosted on Coolify with no per-function deploy-frequency telemetry, so byte-volume is used as a defensible proxy (larger functions tend to span more code paths and thus more potential PII-exposure surfaces). For each sampled function, scanned `console.{log,info,warn,error,debug}` calls for the patterns `email`, `user.id`, `userId`, `portalId`. Cross-referenced against the pseudonymisation utilities in `supabase/functions/_shared/logger.ts` (`maskEmail` at line 29; IP-octet mask helper).

Findings

Function	Raw email/user.id in logs	maskEmail use	Notes
`analyze-properties`	0	0	clean — uses portalId only, treated as non-sensitive identifier per inventory row 3
`pipeline-settings`	0 (only `portalId`)	0	4 `portalId` log lines; consistent with inventory row 3 (quasi-PII, not masked)
`workflows-analyze`	0	0	clean
`mollie-webhook`	0	2	uses maskEmail when email is logged
`hubspot-auth`	0	0	clean
`security-incident`	0	0	clean
`mollie-create-payment`	0	0	clean
`customer-analytics`	0 (only `portalId`)	0	1 `portalId` log; consistent with row 3
`spot-check-accounts`	0	0	clean
`portal-benchmarks`	0	0	clean
`hubspot-users-analytics`	0	0	clean
`create-hubspot-property`	0	0	clean
`rollback-hubspot-operations`	0	0	clean
`predictive-data-quality-alerts`	0	0	clean
`portal-repair`	0	0	clean
`mollie-get-latest-checkout-status`	0	0	clean
`hubspot-health-check`	0	0	clean
`detect-portal-properties`	0	0	clean
`delete-hubspot-property`	0	0	clean
`contact-lifecycle`	0	0	clean

Summary

Findings: 0 log-leaks detected.

Hetzner-managed Nginx access logs

Per NordScope's documented operational-discipline escalation procedure (NDA counterpart): NordScope does NOT have direct control over Coolify-managed Nginx access log retention. Documented limitation; mitigation is upstream config tightening (custom `log_format` omitting sensitive query params) plus the Hetzner support escalation procedure.

Verification gaps (open at time of authoring)

The following verification steps were open when this inventory was authored:

Item	Reason	Resolution path
Direct `auth.users` column verification via live database	Production database access requires per-invocation founder approval	Verify when the schema-drift CI guard runs against the live snapshot, or in a dedicated approved session
24 `trackEvent` call-site enumeration vs an earlier "16 event types" estimate	The estimate predates several event additions	Reconcile against the `Privacy.tsx` analytics disclosure

Last review

Field	Value
Document	PII inventory
Owner	Founder (NordScope)
Cadence	Annual + per-release for PII-bearing schemas
Last reviewed	2026-04-30
Next review due	2026-Q4