Hubswire — Privacy Policy

Effective Date: 2026-05-23 **Version:** 1.0

Hubswire LLC ("**Hubswire**," "**we**," "**us**," "**our**") provides an email management and collaboration platform for customs brokers, freight forwarders, and logistics teams (the "**Service**"). This Privacy Policy explains what personal information we collect through the Service, how we use it, who we share it with, and the rights you have.

This Policy applies to anyone whose personal information passes through the Service, including:

- **Customer end users** — employees of a business that has subscribed to Hubswire (the "**Customer**") who log into and use the Service through their work account.
- **Email correspondents** — third parties whose email messages, contact details, or attachments flow into the Service because they email or are emailed by a Customer end user.
- **Website visitors** — anyone visiting `hubswire.com`, `app.hubswire.com`, or other Hubswire-operated public web pages.

If you are a Customer end user, your employer (the Customer) is the **controller** of the personal information you process through the Service; Hubswire acts as the **processor** on the Customer's behalf. The Customer's own privacy notice governs how it uses your information. Sections below clarify which role applies to each processing activity.

---

1. Information We Collect

1.1 Information You Provide Directly

- **Account information.** When the Customer is provisioned, Hubswire receives the end user's name, work email address, role/title (where supplied), time zone, and authentication identifiers (Microsoft 365 / Azure AD object IDs).
- **Profile and preferences.** Display name, avatar, language, theme, notification settings, snooze defaults, and similar in-app preferences.
- **User-generated content.** Email drafts, comments, mentions, tags, message templates, scheduled-send queues, automation rules, and any other content you author inside the Service.
- **Support communications.** When you contact `support@hubswire.com` (or any equivalent support channel), we receive your name, email, the contents of your message, and any attachments you choose to send.

1.2 Information We Collect Automatically From Your Use of the Service

- **Usage and event data.** Pages and views accessed, actions taken (e.g., archive, snooze, send, assign, comment), feature toggles, timestamps, and inbox/workspace context. Used for product analytics, performance monitoring, and abuse detection.
- **Device and connection data.** IP address, user-agent string, browser/Electron version, operating system, screen resolution, and approximate location derived from IP.
- **Authentication and security logs.** Login timestamps, session identifiers, JWT issuance/refresh events, token-version changes, OAuth callback events, MFA challenges (when initiated by the Customer's identity provider), and failed-access attempts. Retained for security auditing.
- **Cookies and local storage.** We use first-party cookies and browser local storage for session management, CSRF protection, UI preferences (sort order, panel widths, theme), and queued operations (undo windows, draft autosave backups). See **Section 7** for details.

1.3 Information We Receive From Connected Services

Subject to your authorization (via OAuth grant performed by the Customer's admin or end user), Hubswire connects to and ingests data from:

- **Microsoft Graph (Office 365 / Microsoft 365).** Email messages (headers, body, attachments), mailbox folders, calendar events (when scheduling features are enabled), contacts, and the authenticated user's basic profile. Read/write scope necessary for the Service to function as an email client (sync, send, archive, delete on the user's behalf).
- **Front App (optional integration).** Conversations, comments, assignees, and teammate identifiers — used to mirror activity bidirectionally when the Customer has connected a Front workspace.
- **Tracking and logistics providers** (OpenTrack, Terminal49, project44, SeaRates, MarineTraffic, PortPro, and similar). Container, master bill, AWB, vessel, and shipment status data — looked up on demand based on identifiers parsed from email content.
- **Customer-operated ERP gateway.** Read-only query results from the Customer's on-premises Pervasive / Actian Zen database — flowing through an on-prem agent the Customer installs, over an authenticated WebSocket to the Hubswire cloud. Hubswire never executes write queries against the Customer ERP outside of the explicit "document upload" action invoked by an authorized end user.

1.4 Information About Email Correspondents

When a Customer end user sends, receives, or processes email through the Service, the Service necessarily stores the personal information contained in those messages — including the names, email addresses, signatures, and message bodies of third parties who communicate with the Customer's end users. This information is processed under the Customer's instructions; Hubswire acts as the processor and does not use it for its own purposes other than to provide and improve the Service as permitted by the **Data Processing Agreement** ("DPA").

2. How We Use Information

We use the information described above for the following purposes:

PURPOSE	CATEGORIES OF DATA	LEGAL BASIS (GDPR)
Provide, maintain, and operate the Service (email sync, sending, threading, search, collaboration, tracking, ERP visibility, AI features)	Account, content, device, connected-service data	Performance of contract (Art. 6(1)(b)); processor under Art. 28 for Customer-side processing
Authenticate users, manage sessions, enforce CSRF, rate limiting, and access controls	Authentication and security logs, device data	Performance of contract; legitimate interests (Art. 6(1)(f)) — security of the Service
Detect, prevent, and respond to abuse, fraud, malware, phishing, spam, and security incidents	Security logs, content metadata, IP address	Legitimate interests; legal obligation (Art. 6(1)©) where breach notification is required
Generate AI-powered features (Smart Reply, Smart Follow-up, Summarization, Daily Briefing, Recurring Asks, Sentiment, Leader Pulse, Chat)	Email content (truncated, signature-stripped), user prompts, conversation context	Processor under Art. 28 acting on Customer instructions; see **Section 4 (Sub-processors)** for AI providers
Provide product analytics and operational telemetry	Usage events, performance metrics, error reports	Legitimate interests — product improvement
Communicate with the Customer's admins and end users about service availability, security incidents, billing, and product updates	Account information, email address	Performance of contract; legitimate interests
Respond to support requests	Support communications, account information	Performance of contract
Comply with legal obligations (tax, accounting, response to lawful requests)	Account, billing, content as legally required	Legal obligation
Enforce our Terms of Service and protect our rights	All data categories as needed	Legitimate interests

We do **not** sell personal information. We do not "share" personal information for cross-context behavioral advertising as defined by the California Consumer Privacy Act (CCPA) as amended.

3. AI Features — How Email Content Is Handled

The Service includes several AI-powered features that send email content to large-language-model providers for inference. The following rules govern all AI processing:

- **Provider routing.** AI requests are routed to a single provider per request (Google Gemini or OpenAI), selected by Hubswire's SuperAdmin in `/admin/ai-settings`. The default is OpenAI `gpt-4o-mini` for fast tasks and Google Gemini 2.5 Pro for heavier tasks.
- **No training on Customer data.** Hubswire's contracts with Google and OpenAI prohibit those providers from using API-submitted content to train their foundation models. Both providers offer enterprise / API-tier terms that exclude training; we use those tiers exclusively.
- **Content minimization.** Where the prompt does not require the full email (e.g., sentiment classification), Hubswire transmits a truncated, signature-stripped excerpt. Where the full body is needed (e.g., Smart Reply), the body is sent with sender signatures algorithmically removed before transmission.
- **Retention at provider.** Inference requests may be retained by the AI provider for a short window (typically 30 days) for abuse monitoring, per the provider's API terms. Hubswire does not direct the provider to retain content beyond that window.
- **Opt-out.** A Customer can disable AI features at the company level via SuperAdmin support request (`support@hubswire.com`). Per-end-user opt-out is on the roadmap.

4. Sub-processors

Hubswire engages the following sub-processors to deliver the Service. Each is bound by a written agreement that imposes data protection obligations no less protective than this Privacy Policy and the DPA. The current authoritative list lives at `https://hubswire.com/sub-processors` (also reproduced in DPA **Schedule 1**) and is updated when sub-processors change.

SUB-PROCESSOR	PURPOSE	LOCATION
Microsoft Azure (Compute, App Service, PostgreSQL Flexible Server, Managed Redis)	Application hosting, primary database, queue/cache	United States (East US 2)
Microsoft Azure Storage (Blob)	Email attachments, inline images, software installers, auto-update artifacts	United States (East US 2)
Microsoft Graph	Email/calendar synchronization with Customer's Microsoft 365 tenant	United States (Customer's M365 region)

SUB-PROCESSOR	PURPOSE	LOCATION
Google LLC (Gemini API)	AI inference for summarization, sentiment, classification, follow-up	United States
OpenAI, L.L.C.	AI inference for Smart Reply, classification, chat	United States
Hostinger International, Ltd. (SMTP)	Outbound transactional email (notifications, password resets, leader pulse digests) from `notifications@hubswire.com`	European Union
OpenTrack, Inc.	Ocean container and vessel tracking lookups (on-demand)	United States
Terminal49, Inc.	Container tracking and terminal-availability lookups (on-demand)	United States

The Customer is notified at least **30 days in advance** of any addition or replacement of a sub-processor (DPA §4); the Customer has the right to object as described in the DPA.

---

5. How We Share Personal Information

We share personal information only as follows:

- **With sub-processors** (listed in Section 4) for the purposes described.
- **With the Customer.** Personal information of end users is by definition shared with the Customer who provisions and administers their account.
- **With other end users in the same Customer workspace.** In the ordinary course of using collaborative features (assignments, comments, mentions, shared inboxes, delegations, leader-pulse summaries), end users will see each other's names, actions, comments, and (subject to delegation/leader settings) email contents.
- **With professional advisors and corporate transactions.** Auditors, lawyers, accountants, and prospective acquirers in connection with a financing, merger, acquisition, sale of assets, or due-diligence process — subject to confidentiality.
- **In response to lawful requests.** Subpoenas, court orders, government investigations, or where required by law. We will notify the Customer in advance when permitted to do so.
- **To protect rights and safety.** Where we believe disclosure is necessary to investigate fraud, enforce our agreements, or protect the rights, property, or safety of Hubswire, our users, or the public.

We do **not** sell personal information, and we do **not** disclose personal information for cross-context behavioral advertising or for any monetary or other valuable consideration outside the categories above.

6. International Data Transfers

Hubswire is headquartered in the United States and stores Service data primarily in **U.S. Azure regions** (East US 2). When personal information of end users or correspondents located in the European Economic Area, United Kingdom, or Switzerland is transferred to the United States or other third countries, we rely on the following safeguards:

- **Standard Contractual Clauses** (Module 2 — Controller to Processor, and Module 3 — Processor to Sub-processor) as approved by the European Commission, incorporated by reference into the DPA.
- **UK International Data Transfer Addendum** to the SCCs (for transfers from the UK).
- **Swiss FDPIC-approved Clauses** (for transfers from Switzerland) where applicable.

Hubswire performs a Transfer Impact Assessment for each transfer flow on request from a Customer and supplies supplementary technical measures (encryption at rest with AES-256-GCM, encryption in transit with TLS 1.3, access controls) detailed in **DPA Schedule 2**.

7. Cookies and Similar Technologies

The Service uses first-party cookies and browser local storage for the following purposes:

TYPE	PURPOSE	EXPIRY
Authentication	Maintain logged-in session, store JWT (HTTP-only cookie), CSRF state	Session / up to 7 days
Preferences	UI sort order, panel widths, theme (light/dark), draft autosave backups, queued undo operations	Persistent (until cleared)
Security	Rate-limit keys, suspicious-IP tracking	Up to 24 hours
Analytics (first-party only)	In-app event counters for feature-usage telemetry	Aggregated; raw events purged after 90 days

The Service does **not** set third-party advertising or cross-site tracking cookies. Hubswire is a logged-in B2B application; we do not display advertising. Because we do not use cookies for advertising or analytics that require consent under the ePrivacy Directive (beyond strictly-necessary cookies), we do not present a cookie consent banner. End users can disable cookies in their browser settings, but doing so will prevent the Service from functioning.

8. Data Retention

We retain personal information for as long as needed to provide the Service to the Customer, comply with our legal obligations, resolve disputes, and enforce agreements. Specifically:

DATA CATEGORY	RETENTION
Account information (active)	Lifetime of the subscription
Account information (deactivated end users)	90 days after deactivation, then permanently deleted from production systems
Email content (received and sent through the Service)	Lifetime of the subscription; deleted within 90 days after termination per the DPA (subject to legal-hold exceptions)
Authentication and security logs	12 months in production logs, then aggregated or deleted
Application audit logs (`audit_logs` table)	24 months
Support communications	36 months after case closure
Billing records and invoices	7 years (U.S. tax law minimum)
Backups	Encrypted backups retained for up to 35 days (PostgreSQL point-in-time recovery window)
Customs broker–regulated records (where the Customer is a CBP licensee under 19 CFR §111.23)	5 years if the Customer instructs Hubswire in writing to apply a 5-year retention overlay; otherwise, the standard schedule above applies and the Customer is responsible for exporting and retaining required records in its own system of record

After termination, Customer Data is returned or deleted per the DPA. End users may request deletion of personal information at any time per **Section 9**, subject to the Customer's instructions and our legal obligations.

9. Your Rights

Depending on where you live, you may have the following rights with respect to your personal information:

- **Access** — request a copy of the personal information we hold about you.
- **Rectification** — correct inaccurate or incomplete information.
- **Deletion / Erasure** — request that we delete personal information that we are no longer required to retain.

- **Restriction** — limit the way we use your information.
- **Portability** — receive a copy of certain information in a structured, machine-readable format.
- **Objection** — object to processing based on legitimate interests.
- **Withdraw consent** — where we rely on consent, you may withdraw it at any time (without affecting the lawfulness of prior processing).
- **Lodge a complaint** with your local data protection authority.

If you are a Customer end user, please direct rights requests to your employer (the Customer), which controls the processing of your personal information through the Service. The Customer's IT or HR contact can route the request through Hubswire as the processor. You may also contact us directly using **Section 12** and we will route your request to the Customer.

If you are an email correspondent whose personal information appears in a Customer's inbox because of email communication with that Customer, please contact the Customer directly. Hubswire processes your information only on the Customer's behalf and cannot delete it from the Customer's inbox without the Customer's instruction. We will assist the Customer in responding to your request.

For California residents. Under the California Consumer Privacy Act as amended ("CCPA"), you have the right to know, delete, correct, limit use and disclosure of sensitive personal information, opt out of sale or sharing (we do not sell or share), and not be retaliated against for exercising your rights. To exercise these rights, contact `privacy@hubswire.com`.

For EU/EEA/UK/Swiss residents. Hubswire does not maintain an EU establishment; our **Article 27 Representative in the EU** and our **UK Representative** will be designated upon onboarding our first EEA or UK Customer. Until then, please contact `privacy@hubswire.com` for GDPR / UK GDPR requests.

We respond to verified rights requests within 30 days (or such other period as required by applicable law). We may require additional information to verify your identity before fulfilling a request.

---

10. Security

We maintain a security program designed to protect personal information from unauthorized access, disclosure, alteration, and destruction. Measures include:

- **Encryption at rest** — AES-256-GCM for application secrets (OAuth refresh tokens, API keys) via Hubswire's `ENCRYPTION_SECRET`; Azure platform encryption for all storage (PostgreSQL, Blob Storage, Redis).
- **Encryption in transit** — TLS 1.2 minimum (TLS 1.3 preferred) for all client-server traffic and all sub-processor API calls.
- **Access controls** — Role-based access (Super Admin, Company Admin, Member) with least-privilege defaults. Production database access limited to a small set of named operators with MFA-required Azure AD authentication.

- **Authentication** — JWT with short-lived access tokens and token-version revocation; OAuth 2.0 (Microsoft Azure AD) for end-user login; configurable password policy with bcrypt-hashed credentials where password authentication is enabled.
- **Network controls** — Private endpoints between Azure App Service and PostgreSQL/Redis; egress-restricted firewall rules; CORS allowlist enforcement.
- **Application hardening** — CSP enforced on every renderer response (including Electron); CSRF protection via Authorization header requirement on mutating endpoints; rate limiting at the Throttler layer; sanitization of inbound email HTML.
- **Monitoring and alerting** — Real-time alerts (Slack) for token failures, webhook subscription expiry, scheduler outages, reconciliation failures, ERP gateway disconnects, OAuth anomalies. Audit-log retention 24 months.
- **Backups** — PostgreSQL automated backups with up to 35-day point-in-time recovery; geo-redundant Blob Storage replication for attachments.
- **Vendor management** — Sub-processors are vetted for SOC 2 / ISO 27001 attestations; written data-processing addenda are in place with each.
- **Personnel** — All Hubswire personnel are bound by written confidentiality obligations; production access requires explicit authorization.

A complete summary of technical and organizational measures appears in **DPA Schedule 2**. We do not currently hold a SOC 2 attestation; SOC 2 Type I readiness is on our 12-month roadmap (see `Legal/README.md`).

We require sub-processors to notify us of any actual or suspected personal data breach affecting Customer Data without undue delay; Hubswire will notify the Customer **within 72 hours** of becoming aware of a confirmed personal data breach affecting their data (DPA §7).

---

11. Children's Privacy

The Service is a B2B product offered only to commercial businesses. It is not directed to children under the age of 16, and we do not knowingly collect personal information from anyone under 16. If we learn that we have collected such information, we will delete it promptly.

---

12. Contact Us

For privacy questions, requests, or to exercise your rights:

- **Email:** `privacy@hubswire.com`
- **Postal mail:** Hubswire LLC Attn: Privacy 26074 SW 146th CT Homestead, FL 33032 United States

Data Protection Officer: not appointed (Hubswire's processing does not currently require a DPO under GDPR Art. 37; we will appoint one if the legal threshold is met).

13. Changes to This Policy

We may update this Privacy Policy from time to time. Material changes will be communicated to the Customer's admins by email at least **30 days before** taking effect. The "Effective Date" at the top of this page indicates when the current version became effective. Prior versions are available on request.

Changelog

VERSION	EFFECTIVE DATE	SUMMARY
1.0	2026-05-23	Initial publication (pilot customer onboarding).