HUBRIX

# Security & Privacy Whitepaper

Enterprise AI Workspace — Built for European Compliance

| | |
|---|---|
| **Document Version** | v1.0 |
| **Classification** | Public |
| **Effective Date** | May 09, 2026 |
| **Jurisdiction** | European Union (GDPR) |
| **Hosting** | Hetzner Cloud — Helsinki, Finland (EU) |

Issued by Oceanic Consulting VOF | dev@oceanicco.nl | hubrix.ai

# Table of Contents

# 1. Executive Summary

Hubrix is an enterprise AI workspace developed and operated by Oceanic Consulting VOF, a Dutch company registered in the Netherlands. This document describes the security, privacy, and compliance measures implemented to protect customer data and ensure regulatory compliance within the European Union.

**Key Security Commitment:** All customer data is stored exclusively on EU-based infrastructure in Helsinki, Finland. No data is transferred outside the European Economic Area (EEA) without explicit contractual safeguards. Hubrix is designed with GDPR compliance as a foundational requirement, not an afterthought.

| Security Attribute | Status | Details |
|---|---|---|
| Data Residency | **EU-only** | Hetzner Helsinki, FI |
| Encryption at rest | **Enabled** | AES-256 |
| Encryption in transit | **TLS 1.3** | All endpoints |
| GDPR Compliance | **Implemented** | Art. 17, 20, 25, 32 |
| SSO Support | **Active** | Google & Microsoft Entra |
| MFA / 2FA | **Active** | TOTP + Recovery codes |
| Audit Logging | **Active** | All user actions |
| Data Retention | **Configurable** | GDPR-compliant deletion |

# 2. Infrastructure & Hosting

Hubrix operates on Hetzner Cloud infrastructure, one of Europe's largest and most trusted cloud providers, certified under ISO/IEC 27001 and ISO/IEC 27017.

## 2.1 Hosting Details

| | | |
|---|---|---|
| ✓ | **Cloud Provider** | Hetzner Cloud GmbH (Germany) |
| ✓ | **Data Center Location** | Helsinki, Finland (EU/EEA) |
| ✓ | **Server Type** | Dedicated vCPU — CX33 (4 vCPU, 8GB RAM, 80GB NVMe) |
| ✓ | **Provider Certifications** | ISO 27001 \| ISO 27017 \| ISO 27018 \| C5 |
| ✓ | **Network Security** | Cloudflare WAF + DDoS protection on all endpoints |
| ✓ | **DNS & CDN** | Cloudflare (EU privacy zone, no US data transfer) |
| ✓ | **Uptime** | Target 99.5% monthly (single-node; HA in roadmap) |

## 2.2 Network Architecture

All HTTP traffic is proxied through Cloudflare before reaching the application servers. This provides an additional layer of DDoS protection, WAF (Web Application Firewall), and TLS termination. Backend services communicate exclusively over localhost or private network interfaces — no backend port is exposed to the public internet.

## 2.3 Backup & Recovery

- Daily automated backups at 02:00 CET (PostgreSQL full dump + application code)
- Remote backup copy to secondary server (Grafana server, separate datacenter)
- Last 7 daily backups retained locally; last 15 days on remote server
- Database backups use pg_dump with gzip compression (AES-256 at rest)
- Recovery Time Objective (RTO): < 4 hours | Recovery Point Objective (RPO): < 24 hours

# 3. Data Architecture

## 3.1 Data Storage

All customer data is stored in a PostgreSQL 16 database with pgvector extension for AI embeddings. Each company's data is logically isolated using company_id foreign keys enforced at the application layer on every query.

| Data Type | Storage | Isolation Level |
|---|---|---|
| User profiles & auth | PostgreSQL 16 | Company-scoped |
| Chat sessions & messages | PostgreSQL 16 | Company-scoped |
| Documents & RAG embeddings | PostgreSQL + pgvector | Company-scoped |
| File uploads (avatars, exports) | Local filesystem (encrypted) | User-scoped |
| AI provider API keys | PostgreSQL (encrypted) | System-level |
| Session tokens | Redis 7 (in-memory) | User-scoped, TTL 24h |
| Audit logs | PostgreSQL 16 | Company-scoped |
| Stripe billing data | Stripe (PCI DSS Level 1) | Company-scoped |

## 3.2 Data Isolation

Hubrix uses a multi-tenant architecture where all tenants (companies) share the same database instance but are strictly isolated at the application layer. Every database query is scoped to the authenticated user's company_id. Cross-company data access is architecturally impossible without explicit admin privileges.

**Important:** No tenant can access another tenant's data. Company A's chat history, documents, agents, and user data are completely invisible to Company B. This is enforced at every API endpoint through authenticated session validation.

## 3.3 AI Content Processing

When users send messages to AI providers (Anthropic, OpenAI, Google, etc.), the content is transmitted to those providers according to their respective data processing agreements. Hubrix does not store raw AI responses beyond what is displayed in the user interface — all conversation history is stored in our EU database.

# 4. Authentication & Access Control

## 4.1 Authentication Methods

- **Email + Password:** bcrypt hashing (cost factor 12), minimum 8 characters
- **Google SSO:** OAuth 2.0 + OpenID Connect via Google Workspace
- **Microsoft SSO:** OAuth 2.0 via Microsoft Entra ID (Azure AD)
- **TOTP 2FA:** RFC 6238 compliant, compatible with Authenticator apps
- **Recovery Codes:** Argon2-hashed one-time codes for 2FA fallback
- **API Keys:** SHA-256 hashed, scoped permissions, revocable

## 4.2 Role-Based Access Control (RBAC)

| Role | Scope | Capabilities |
|---|---|---|
| Owner | Company | Full access, billing, member management |
| Admin | Company | All features except billing |
| Member | Company | Assigned features based on plan |
| Super Admin | Platform | Hubrix staff only — system administration |

## 4.3 Session Management

- JWT access tokens with 24-hour expiry (configurable)
- Refresh tokens stored server-side, revocable at any time
- All active sessions visible and terminable from user settings
- Force logout available for all sessions (admin and user)
- Rate limiting: 5 failed login attempts triggers temporary lockout
- IP-based rate limiting on all authentication endpoints
- MFA session tokens expire in 5 minutes (single-use)

# 5. Data Encryption

## 5.1 Encryption in Transit

All communication between clients and Hubrix servers uses TLS 1.2 or higher. TLS certificates are automatically provisioned and renewed by Caddy (Let's Encrypt) with a minimum RSA-2048 or ECDSA P-256 key strength.

| | | |
|---|---|---|
| ✓ | **Minimum TLS version** | TLS 1.2 (TLS 1.3 preferred) |
| ✓ | **Certificate Authority** | Let's Encrypt (auto-renewed, 90-day cycle) |
| ✓ | **HSTS** | Enabled — max-age 1 year, includeSubDomains |
| ✓ | **Certificate transparency** | All certs logged to CT logs |
| ✓ | **Internal services** | All backend services on localhost only |

## 5.2 Encryption at Rest

- Hetzner storage volumes are encrypted at the infrastructure level (AES-256)
- Sensitive fields (API keys, OAuth tokens) are encrypted at the application level before storage
- Passwords are hashed using bcrypt (cost factor 12) — never stored in plaintext
- Recovery codes are hashed using Argon2id before storage
- Database backups are compressed and stored with filesystem-level encryption

# 6. GDPR Compliance

Hubrix is designed and operated in full compliance with the General Data Protection Regulation (EU) 2016/679. As a Dutch company, Oceanic Consulting VOF operates under EU jurisdiction and is directly subject to GDPR requirements.

## 6.1 Data Subject Rights

| Right | Article | Implementation |
|---|---|---|
| Right to Access | Art. 15 | Data export available from user settings |
| Right to Erasure | Art. 17 | Account deletion with full data purge |
| Right to Portability | Art. 20 | JSON/CSV export of all personal data |
| Right to Rectification | Art. 16 | Profile editing available at any time |
| Right to Object | Art. 21 | Processing stops upon request |
| Right to Restriction | Art. 18 | Account suspension without data deletion |

## 6.2 Legal Basis for Processing

- **Contract (Art. 6(1)(b)):** Processing necessary to provide the Hubrix service to registered users under the Terms of Service.
- **Legitimate Interest (Art. 6(1)(f)):** Security monitoring, fraud prevention, and service improvement through anonymized analytics.
- **Consent (Art. 6(1)(a)):** Optional features such as marketing communications require explicit opt-in consent.

## 6.3 Data Retention

- Active account data: retained for the duration of the subscription
- Deleted account data: purged within 30 days of account deletion request
- Audit logs: retained for 12 months for security and compliance purposes
- Billing records: retained for 7 years (Dutch tax law requirement)
- Backup data: automatically purged after 15 days

## 6.4 Privacy by Design (Art. 25)

Hubrix implements privacy by design principles: data minimization (only necessary data collected), purpose limitation (data used only for stated purposes), and default privacy settings that protect users

without requiring action on their part.

# 7. AI Provider Security

Hubrix integrates with multiple AI providers. When content is sent to these providers, it is processed according to their respective data processing terms. Hubrix has selected providers that offer enterprise data protection agreements.

| Provider | Data Processing | Training on Data | Region |
|---|---|---|---|
| Anthropic (Claude) | API DPA available | No (with DPA) | US (SCCs apply) |
| OpenAI | API DPA available | No (with DPA) | US (SCCs apply) |
| Google (Gemini) | Google Cloud DPA | No (with DPA) | EU option available |
| DeepSeek | API terms | Review required | CN (review required) |
| xAI (Grok) | API terms | Review required | US |
| Mistral AI | API DPA available | No (with DPA) | EU (France) |

**Customer Control:** Enterprise customers can restrict which AI providers their team members may use. Administrators can disable specific providers from the admin panel, ensuring compliance with internal data handling policies.

# 8. Incident Response

## 8.1 Incident Classification

| Severity | Definition | Response Time | Notification |
|---|---|---|---|
| P1 — Critical | Data breach, service unavailable | < 1 hour | Within 24h |
| P2 — High | Auth issues, data exposure risk | < 4 hours | Within 72h |
| P3 — Medium | Performance degradation | < 24 hours | Next business day |
| P4 — Low | Minor bugs, UI issues | < 72 hours | Monthly report |

## 8.2 GDPR Breach Notification (Art. 33/34)

In the event of a personal data breach, Oceanic Consulting VOF will notify the relevant supervisory authority (Dutch Data Protection Authority — Autoriteit Persoonsgegevens) within 72 hours of becoming aware of the breach, as required by GDPR Art. 33. Affected data subjects will be notified without undue delay where the breach is likely to result in a high risk to their rights and freedoms (GDPR Art. 34).

# 9. Third-Party Sub-processors

Hubrix uses the following sub-processors to deliver its services. All sub-processors are bound by data processing agreements (DPAs) and provide adequate protection for personal data.

| Sub-processor | Purpose | Location | Transfer Mechanism |
|---|---|---|---|
| Hetzner Cloud GmbH | Infrastructure hosting | Germany / Finland (EU) | No transfer needed |
| Cloudflare Inc. | CDN, WAF, DNS | EU (with EU DPA) | Standard Contractual Clauses |
| Anthropic PBC | Claude AI models | United States | Standard Contractual Clauses |
| OpenAI LLC | GPT AI models (optional) | United States | Standard Contractual Clauses |
| Google LLC | Gemini AI + SSO | United States / EU | Standard Contractual Clauses |
| Microsoft Corp. | Entra ID SSO | United States / EU | Standard Contractual Clauses |
| Stripe Inc. | Payment processing | United States | Standard Contractual Clauses |
| Resend Inc. | Transactional email | United States | Standard Contractual Clauses |

# 10. Security Roadmap

Hubrix is committed to continuously improving its security posture. The following certifications and improvements are planned:

| Initiative | Target | Status |
|---|---|---|
| High Availability (HA) deployment | Q3 2026 | In planning |
| Penetration test (external firm) | Q3 2026 | Scheduled |
| SOC 2 Type I audit (via Vanta) | Q4 2026 | **Planned** |
| ISO 27001 gap assessment | Q4 2026 | Planned |
| Customer Audit Log UI | Q2 2026 | In development |
| Granular RBAC (per-feature roles) | Q3 2026 | Planned |
| SSO enforcement (mandatory for Enterprise) | Q2 2026 | Available |
| Data residency selection (per company) | Q4 2026 | Planned |

**Transparency commitment:** Hubrix publishes security updates and significant changes to this whitepaper on docs.hubrix.ai. Enterprise customers are notified of material changes to our security posture via email.

# 11. Contact

## Security Inquiries

For security vulnerability reports, data protection questions, or to request a copy of our Data Processing Agreement (DPA), please contact:

| | |
|---|---|
| **Data Controller** | Oceanic Consulting VOF |
| **Registered address** | Poortugaal, South Holland, Netherlands |
| **Security contact** | dev@oceanicco.nl |
| **Privacy / DPA requests** | dev@oceanicco.nl (subject: DPA Request) |
| **Website** | https://hubrix.ai |
| **API & Technical docs** | https://api.hubrix.ai \| https://docs.hubrix.ai |

This document is reviewed and updated annually or upon significant changes to our security practices. Version 1.0 | May 2026 | Oceanic Consulting VOF