

Power Belt Security Overview

Document version: 2.2

Date: 14 October 2025

Contact: hello@power-belt.cz

Company: Power Nodes s.r.o.

Responsible Security Contact: Ing. Marek Nový — Head of IT/ISMS

1. Introduction

Power Belt is a **cloud-based Lean Six Sigma & DMAIC analysis tool** developed by Power Nodes s.r.o. It helps companies optimize business processes through:

- advanced analytics
- video analysis via **Lean Player**
- AI-powered guidance

This overview describes Power Belt's approach to cybersecurity and data protection, mapped to ISO 27001 principles, GDPR, and NIS2 readiness.

2. Hosting & Architecture

Item	Details
Type	SaaS, multi-tenant
Hosting provider	Supabase (runs on AWS / GCP per region)
Primary data location	EU data centers — Frankfurt or Amsterdam
Tech stack	NextJS · PostgreSQL (database) · Supabase (auth & storage)

3. Access Control & Identity Management

- **Authentication methods**
 - Email + password (strong password policy)
 - *Optional* SSO (SAML / Entra ID)
- **Authorization** — Role-based access control (**RBAC**)
- **Session handling** — short-lived Access + Refresh tokens (OAuth 2.0)
- **Account isolation** — one user = one licence; concurrent-login prevention

4. Data Security

Control	Implementation
Encryption at rest	AES-256 (managed DB encryption)
Encryption in transit	TLS 1.2 / 1.3 for all client-server traffic
Back-ups	Automated daily; 30-day retention; off-site replicas
Data retention & deletion	Customer-controlled; automatic purge after 2 years of inactivity or on request
Video files	Remain in the user's browser — never stored or processed server-side except AI analysis

5. AI Video Analysis

Power Belt ensures secure handling of all video files during AI analysis through controlled access, short retention, and encrypted transfer.

5.1. Controlled Access

Users upload videos directly to Supabase Storage with authentication. Each file is tied to the uploader and protected by Supabase Row-Level Security (RLS).

5.2. Authorized Processing

When AI analysis is triggered, Power Belt sends a short-lived Supabase access token to the Transcoding Server. The server uses this token to securely pull only the user's uploaded files.

5.3. Temporary Retention

Video files and analysis data are retained only as long as necessary for processing:

Files remain in Supabase Storage and Google Vertex AI for a maximum of 48 hours, after which they are automatically deleted.

Vertex AI caching is enabled to optimize inference performance and reduce latency. Cached data (prompts and outputs) is automatically purged within 24 hours, in accordance with Google's caching policy.

No video data is used by Google for model training, tuning, or improvement

5.4. Secure Transmission

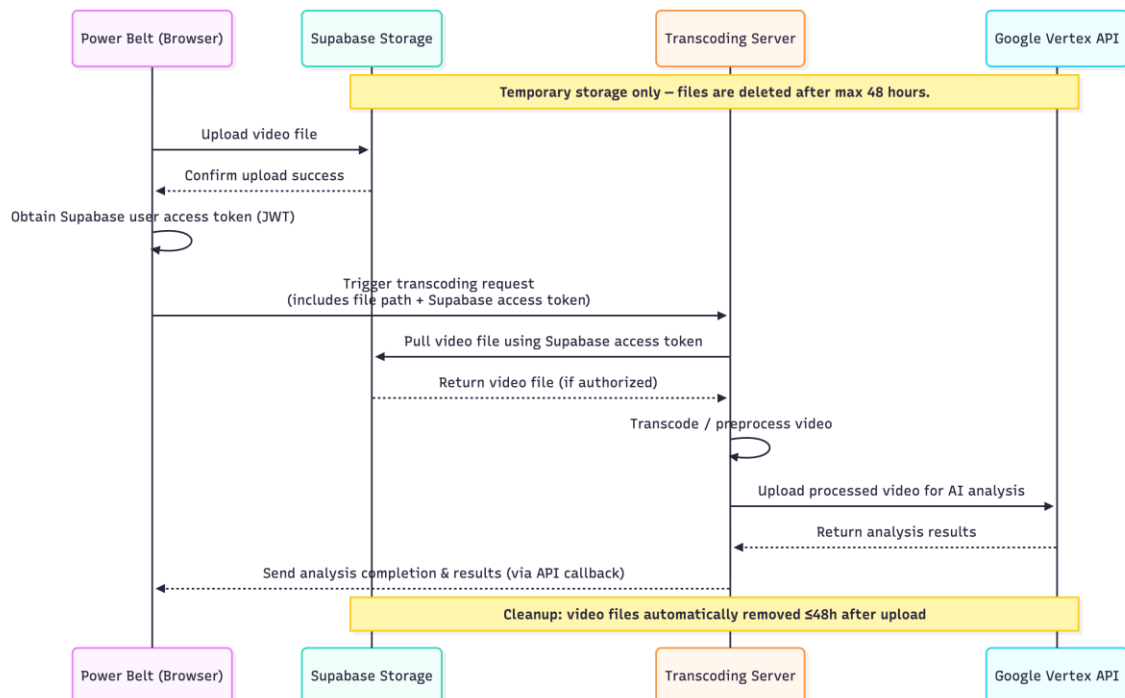
All communication between Power Belt, Supabase, the Transcoding Server, and Google Vertex AI uses TLS-encrypted HTTPS connections. Access tokens are never logged or stored in URLs.

5.5. Logging & Compliance

Each access and deletion event is logged with user and file identifiers. All services follow least-privilege access principles and comply with data minimization standards.

5.6. Google Vertex AI Zero-Retention Configuration

Google Vertex AI services are operated in accordance with Google's Zero Data Retention Policy, ensuring that any cached data is automatically deleted within 24 hours and never used for model training.



6. Vulnerability Management

- **Patch management** — dependencies tracked by automated tooling (Dependabot)

- **Secure coding** — aligned with OWASP Top 10
- **Dependency scanning** — every build validated for vulnerabilities before deployment

7. Monitoring & Logging

- **Audit trails** — log logins, project access, edits, and other key actions
- **Monitoring stack** — LogRocket + backend telemetry
- **Anomaly detection** — alerts on:
 - concurrent logins
 - unusual data-volume access
 - other suspicious behaviour

8. Incident & Breach Management

1. **Incident response plan** — documented and regularly tested
2. **Notification** — customers informed within **72 hours** of a confirmed breach
3. **Post-incident review** — root-cause analysis and preventive actions captured

9. Compliance Status

Framework	Status	Notes
GDPR	✓ Compliant	Supports export, deletion, consent management
NIS2	⚙ In progress	Architecture & processes already aligned
ISO 27001	⌚ Not yet certified	Controls mapped; formal certification planned

10. Physical Security

- **Cloud-only infrastructure** — no on-prem data centers
- **Endpoint policy** — full-disk encryption, strong passwords, remote-wipe capability on all dev & support devices

11. Third-party Risk Management

- **DPA**s in place with all service providers (e.g., Supabase)
- **Sub-processor list** — available on request, including security commitments

12. Summary

Power Belt maintains a **robust security posture** aligned with industry standards and best practices. While ISO 27001 certification is pending, equivalent controls are already implemented and continually improved to meet demanding enterprise requirements.