

MySalaryPal — Security & Data Handling

Employee payslip portal · Prepared for prospect IT / Information Security teams · v1.0

Hosting & Data Residency

- Application hosted on Cloudflare's EU edge network (workerd runtime); TLS 1.2+ enforced end-to-end.
- Database, authentication and file storage on Supabase (managed Postgres) in the EU region (Ireland / Frankfurt).
- All personal data of EU/UK employees remains within the EEA. No data is processed in the US.
- Subprocessors: Cloudflare (EU), Supabase (EU), Paddle (billing only, no payslip data), Google (OAuth only, optional).

Access Control & Tenancy

- Row-Level Security (RLS) enabled on every table in the public schema — enforced by Postgres, not by app code.
- Each company is an isolated workspace; employees can only read rows scoped to their own user_id; admins are scoped to their company_id.
- Roles stored in a dedicated user_roles table with a SECURITY DEFINER has_role() function — prevents privilege escalation.
- Authentication: email + password, Google SSO, and SAML SSO (enterprise). Passkeys (WebAuthn / Face ID / Touch ID) supported as a second factor.
- Admin operations gated by server-side role checks; service-role keys never exposed to the browser.

Audit & Tamper Evidence

- Immutable audit log of all admin actions: payslip delivery/deletion, member invites/removals, branding changes, broadcasts, passkey events.
- Each row is SHA-256 hash-chained to the previous row (prev_hash → row_hash) — any retroactive edit breaks the chain.
- Admins can verify the full chain in-app and export a tamper-evident JSON bundle for auditors at any time.
- Audit log retained for the life of the workspace; CSV export available on demand.

GDPR & Data Subject Rights (Self-Serve)

- Every employee can export all their data (profile, payslips, anomalies, pension records, audit trail, devices) as a JSON bundle from their Security page — no ticket required.
- Account & data deletion available on request via the workspace admin or security@mysalarypal.com; processed within 30 days per GDPR Art. 17.
- Data Processing Agreement (DPA) available at mysalarypal.com/legal/MySalaryPal-DPA.pdf; DPIA template provided to assist customer assessments.
- Privacy policy, terms, and trust page published at mysalarypal.com/privacy, /terms, /trust.
- Lawful basis: contract (Art. 6(1)(b)) between customer (controller) and MySalaryPal (processor); employees are data subjects of the customer.

Application Security

- All input validated server-side with Zod schemas; parameterised queries throughout (no raw SQL from user input).
- Webhooks (Paddle billing, cron jobs) verified with HMAC-SHA256 signatures and timing-safe comparison.
- Cloudflare Turnstile CAPTCHA on public sign-up and demo request forms; rate-limiting on auth endpoints.
- Secrets (service keys, webhook secrets, VAPID keys) stored in the platform secret manager; never committed to source control.
- Responsible disclosure policy published at /.well-known/security.txt; contact: security@mysalarypal.com (2 business day acknowledgement).

Operational & Compliance Roadmap

- Encryption: in transit (TLS 1.2+) and at rest (AES-256, managed by Supabase & Cloudflare).
- Backups: automated daily Postgres backups with point-in-time recovery (7-day window) provided by Supabase.
- Incident response: breach notification to customer DPO within 72 hours per GDPR Art. 33.
- Penetration test & SOC 2 Type II / ISO 27001 audit planned post-pilot — current security architecture is designed to support these certifications without rework.

Security contact security@mysalarypal.com	Trust & policies mysalarypal.com/trust	DPA mysalarypal.com/legal/MySalaryPal-DPA.pdf
---	--	---

MySalaryPal (MSP) is operated by the MySalaryPal team. This document summarises current security posture as of the date of issue and is provided to assist prospective customers' IT & InfoSec review. It is not a contractual commitment; binding terms are set out in the Master Services Agreement and DPA.