# TPSClear Security Overview

**August 2026. Offered in lieu of an ISO 27001 certificate; see section 11 for our certification position.**

## 1. Company profile

TPSClear (tpsclear.co.uk) is a UK Telephone Preference Service (TPS) and Corporate TPS (CTPS) phone number screening service operated by Voll Studios Ltd, a company registered in England and Wales (company number 09302803, registered office 5 Brayford Square, London, England, E1 0SG). Voll Studios Ltd is registered with the Information Commissioner's Office under registration ZC135838.

Production access is deliberately concentrated in one person, the founder and director. That shapes the security model honestly described in this document: exactly one privileged user, no shared accounts, no third-party contractors with production access, and no offboarding surface. External professional advisers (accountancy) support back-office functions under engagement terms that include confidentiality; they have no access to production systems or customer data. Where a control normally implies a team (segregation of duties, peer review), we say so plainly rather than claim otherwise.

## 2. Architecture summary

- **Application:** Next.js, hosted on Vercel (serverless functions and edge network; UK and EU traffic served from EU regions). The public API is served at api.tpsclear.co.uk over HTTPS only.
- **Database:** Supabase managed Postgres, hosted in an EU region. Row-level security is enabled on all application tables; access is server-side only via a scoped service key. There is no client-side or anonymous database access path.
- **Screening:** live register lookups are performed by UK-based licensed data partners (Data8 and Selectabase) via authenticated server-to-server calls. TPS/CTPS register data is sourced under licence through these partners.
- **Billing:** Stripe. Card data is handled entirely by Stripe; it never touches TPSClear systems.
- **Email:** Resend for transactional service email; Google Workspace for business correspondence.
- **CRM integrations:** the TPSClear HubSpot app runs inside the customer's own HubSpot portal and writes verdicts to the customer's own CRM records. HubSpot is the customer's environment, not a TPSClear sub-processor.

## 3. Data handled

**What we process:** UK telephone numbers submitted for screening (normalised to E.164), the resulting verdicts (Clean, TPS-listed, CTPS-listed, Unknown) with timestamps, CRM record identifiers,

optional customer-supplied campaign references, and the account and authentication records needed to run the service (API key hashes, OAuth installation records, billing contact details).

**What we do not process or store:**

- No names, addresses, or emails attached to the numbers being screened; the screening operation works on the number alone.
- No card or bank details (held by Stripe).
- No raw IP addresses in our database; requesting IPs are stored only as salted SHA-256 hashes.
- No telephone numbers in telemetry or error logs; operational logging records timestamps, error codes, and usage counts only.

**Where screening data lives:** verdicts are returned in the API response or written to the customer's own CRM. Server-side, a verdict cache (number plus verdict) allows repeat screenings within 28 days without a fresh paid lookup and is cleared within 60 days, and each API request produces an audit record (retained up to 12 months) so customers can evidence screening for PECR compliance via the returned X-Request-Id.

## 4. Access control

- Production access is held by exactly one named individual (the founder and director); no shared accounts. Least privilege holds by construction, and there is no joiner, mover, or leaver surface.
- Multi-factor authentication is enabled on all administrative accounts (hosting, database, billing, registrar, and email provider consoles).
- Production services use per-provider scoped credentials (dedicated database service key, per-service API keys) rather than any master credential; secrets are held in the hosting platform's encrypted environment configuration, not in source control.
- Customer API keys are issued per environment (test and live), stored only as SHA-256 hashes, verified in constant time, and can be revoked or rotated at any time.

## 5. Encryption

- In transit: TLS 1.2 or higher on every connection, including server-to-server calls to data partners and sub-processors. HSTS is enforced with a two-year max-age, includeSubDomains, and preload.
- At rest: the managed database and hosting platforms encrypt stored data at rest.

## 6. Network and application security

- Baseline HTTP security headers on every route: Strict-Transport-Security, X-Content-Type-Options: nosniff, Referrer-Policy: strict-origin-when-cross-origin, X-Frame-Options: DENY, a Permissions-Policy denying camera, microphone, geolocation and browsing-topics, and a Content-Security-Policy restricting object-src, base-uri, and frame-ancestors.

- Rate limiting throughout: weighted per-key lookup budgets enforced atomically in the database, per-IP and global caps on public form endpoints, and per-portal daily screening caps on CRM integrations.
- Input hardening: request bodies capped (16 KB on forms, 64 KB on the screening endpoint), screening batches capped at 1,000 numbers, strict server-side validation with field length limits and allowlists, and anti-automation measures on public forms.
- Fail-safe screening: a register-provider failure is never reported as Clean; affected numbers return as Unknown so a customer cannot be misled into calling an unscreened number.
- Webhook payloads from integrated platforms are signature-verified before processing.

## 7. Vulnerability and dependency management

- Dependencies are kept current and patched as advisories emerge.
- The hosting platform's deployment pipeline blocks any release whose production dependencies carry known high-severity security advisories, so a vulnerable dependency cannot reach production.
- No external penetration test has been commissioned to date; we will cooperate with customer-initiated security testing by arrangement.

## 8. Logging and monitoring

- Automated daily operational checks verify production availability and payment-webhook delivery, with alerts routed directly to the operator.
- An automated daily anomaly check reviews security-event counters (authentication failures, rate-limit trips, anti-automation triggers, screening-cap breaches) and alerts the operator when counts cross defined thresholds. The counters hold aggregate counts only, no request data or personal data.
- Platform function logs and error traces (retained around 30 days) support incident investigation. Telephone numbers are excluded from these logs.
- Screening API calls produce per-request audit records referenced by the X-Request-Id returned to the customer.

## 9. Incident response and breach notification

The operator is directly responsible for incident response; there is no handoff chain. On becoming aware of a personal data breach affecting customer data we will notify affected customers without undue delay, and in any event within 48 hours, with the details available at that time (nature of the breach, data and data subjects concerned, likely consequences, and mitigation), updating as the investigation progresses. As a controller we notify the ICO within 72 hours where the UK GDPR threshold is met. These commitments are contractual in our Data Processing Agreement.

## 10. Data retention and deletion

- Screening verdict cache: reused for up to 28 days, deleted within 60 days of the underlying check.
- Screening audit records: up to 12 months, then deleted.
- Operational telemetry (timestamps, error codes, usage counts): up to 12 months, then deleted or fully anonymised.
- Platform function logs: hosting platform defaults, typically around 30 days.
- Account records: life of the account plus 12 months after closure, unless law requires longer.
- On termination, customer data is returned or deleted within 30 days at the customer's choice, per the DPA.

## 11. Certifications and compliance position

- Voll Studios Ltd holds **no ISO 27001 certification and no SOC 2 report**. At our current scale we consider a full ISMS certification disproportionate; this document, together with our DPA and privacy policy, describes the controls actually in place.
- **ICO registered:** ZC135838.
- We operate UK GDPR compliant practices as described here and in our DPA: documented processing purposes, data minimisation, defined retention, sub-processor contracts with UK transfer mechanisms, and breach notification commitments.
- Our infrastructure sub-processors (Vercel, Supabase, Stripe, Cloudflare, Google) maintain their own ISO 27001 and/or SOC 2 programmes; their certifications cover the physical and platform layers of the service.

## 12. Sub-processors

The HubSpot platform is excluded below because the TPSClear app runs inside the customer's own HubSpot portal (the customer's environment, under the customer's HubSpot agreement).

| Sub-processor | Service | Data processed | Location / region | Transfer mechanism |
|---|---|---|---|---|
| Vercel Inc. | Application hosting, serverless API, edge network, web analytics | All data passing through the service; platform logs | US company; UK and EU traffic served from EU regions | UK Addendum to the EU SCCs (Vercel DPA) |
| Supabase, Inc. | Managed Postgres database | Verdict cache, audit records, account and installation records, hashed request metadata | US company; database in an EU region | EEA data at rest (UK adequacy); UK Addendum (Supabase DPA) |

| Sub-processor | Service | Data processed | Location / region | Transfer mechanism |
|---|---|---|---|---|
| Selectabase Ltd | Licensed TPS/CTPS screening provider (register lookups) | Telephone numbers submitted for live screening | United Kingdom | Not applicable (UK processing) |
| Data8 Ltd | Licensed data partner for TPS/CTPS register data | Telephone numbers submitted for screening, where this partner performs the lookup | United Kingdom | Not applicable (UK processing) |
| Stripe, Inc. (and Stripe Payments Europe Ltd) | Payments and subscription billing | Billing contact details only; no screening data | US / Ireland | UK Addendum / SCCs (Stripe DPA) |
| Resend, Inc. | Transactional email | Account holder names and email addresses; no screening data | United States | UK Addendum / SCCs (Resend DPA) |
| Cloudflare, Inc. | DNS and email routing for tpsclear.co.uk | Mail routing metadata | US company, global network | UK Addendum / SCCs (Cloudflare DPA) |
| Google (Google Ireland Ltd) | Business email (Workspace); marketing-site analytics (GA4, consent denied by default) | Support correspondence; aggregate, cookieless site analytics | Ireland / EU, possible US processing | UK adequacy (EEA); UK Addendum (Google DPA) |

## 13. Continuity and customer exit

We address key-person risk through low dependency rather than headcount:

- **The platform runs without operator intervention.** Hosting, database, DNS, billing, and the daily retention jobs are managed services that continue operating unattended; there is no server anyone needs to log into to keep the service up.
- **Customer exposure is shallow by design.** TPSClear is a screening layer, not a system of record. The customer's CRM data stays in the customer's own HubSpot portal; we hold only short-lived screening verdicts (28-day cache) and a 12-month audit log, both of which expire automatically.
- **Exit is straightforward.** Subscriptions are monthly with no lock-in. On termination the DPA requires return or deletion of customer data, and the automated retention schedule deletes it regardless.

- **Code and configuration are fully reproducible** from version control, so the service can be rebuilt or handed over from the repository alone.

Questions about this document: privacy@tpsclear.co.uk. The current version is available on request, and material changes to the sub-processor list are notified to active customers in advance.