# Data Protection Impact Assessment: TPS/CTPS Screening Service

**Voll Studios Ltd (trading as TPSClear), August 2026. Conducted voluntarily; reviewed annually or before any material change to processing.**

## 1. Why this DPIA exists

Voll Studios Ltd (company number 09302803, ICO registration ZC135838) operates TPSClear, a UK Telephone Preference Service (TPS) and Corporate TPS (CTPS) screening service. For screening, TPSClear acts as a **processor** on the instructions of its customers, who are controllers of the telephone numbers they submit. The formal Article 35 DPIA duty for high-risk processing sits with the controller; this assessment is conducted voluntarily so that (a) customers' own DPIAs can draw on it, and (b) the company has evidence that the processing has been assessed against UK GDPR requirements. The assessment follows the ICO's DPIA framework: describe, assess necessity, identify risks, identify mitigations, sign off.

## 2. Description of the processing

**Nature.** Customers submit UK telephone numbers (via REST API or the TPSClear HubSpot app). Each number is normalised to E.164 and checked against the statutory TPS/CTPS registers through UK-licensed data partners (Data8, Selectabase). The verdict (Clean, TPS-listed, CTPS-listed, Unknown) is returned to the customer and, for CRM integrations, written to the customer's own CRM record.

**Scope of data.** The telephone number alone, with no attached names, addresses, or emails. Also processed: CRM record identifiers, optional customer campaign references, timestamps, and salted SHA-256 hashes of requesting IPs. Verdicts are cached for reuse up to 28 days (deleted within 60); per-request audit records are retained 12 months so customers can evidence PECR compliance; no numbers appear in telemetry or error logs.

**Context.** Data subjects are the customer's contacts. They have registered (or not) with statutory do-not-call registers; screening gives effect to that registration. Processing volume is bounded by per-customer caps and rate limits.

**Purpose.** To enable customers to comply with regulation 21 PECR (the prohibition on unsolicited marketing calls to TPS/CTPS-registered numbers) before dialling.

## 3. Necessity and proportionality

- **Lawful basis** is the controller's to establish; typically legitimate interests in complying with PECR. TPSClear processes strictly under the DPA and customer instruction (Article 28).
- **Necessity.** A number cannot be screened against the registers without processing the number. No lesser data achieves the purpose.

- **Data minimisation is structural.** The service refuses by design to take more than the number: no names, no addresses, no enrichment, no profiling. Verdict plus timestamp is the entire output.
- **Retention is bounded and enforced in code** (28-day reuse cache deleted within 60 days; 12-month audit records; automated daily retention job).
- **No automated decision-making with legal effect on data subjects**: the verdict informs whether the customer may lawfully call; it is the register's status, not a judgement about the person.

## 4. Risks to data subjects, and mitigations

| # | Risk | Severity / likelihood | Mitigations |
|---|---|---|---|
| 1 | Wrong verdict of Clean leads to an unwanted call to a TPS-registered person | Low harm, low likelihood | Register lookups via licensed partners against the statutory registers; fail-safe design: any provider failure returns Unknown, never Clean; 28-day cache cap keeps verdicts fresh against re-registration |
| 2 | Breach of the number store enables linkage or misuse | Low harm (numbers without identities), low likelihood | Server-only database access behind a scoped service key with RLS enabled; TLS 1.2+ everywhere; encrypted at rest; no client-side database path; numbers excluded from logs and telemetry |
| 3 | Function creep: numbers reused beyond screening | Low likelihood | Contractually barred by the DPA; no secondary use, no resale, no model training; structural absence of identity data limits value of any misuse |
| 4 | Retention beyond need | Low | Retention enforced by automated daily job, not manual practice; deletion on customer exit per DPA within 30 days |
| 5 | Sub-processor transfer risk (US-parent cloud providers) | Low | EU-region hosting for application and database; UK Addendum / SCCs with each sub-processor; sub-processor list published with advance notice of changes |

Residual risk after mitigations is assessed as **low**. The processing gives effect to data subjects' own registered preferences, and the service holds less data about them than any alternative compliance route (manual register checks or bureau list-washing with full contact records).

## 5. Consultation and sign-off

No prior consultation with the ICO is required: the processing is not high-risk after mitigation. Data subject consultation is impractical for a processor with no relationship with them; their interests are represented by the statutory register scheme itself. This assessment was conducted and approved by the company director as the accountable owner.

**Outcome: processing may proceed. Next review: August 2027, or before any material change** (new data categories, new register sources, any move away from the number-only model).

Questions: privacy@tpsclear.co.uk