Data Processing Agreement

Version 1.0 · Last updated 16 June 2026

This DPA is incorporated by reference into the CleanDupTool Terms of Service. By uploading CRM data containing personal data into CleanDupTool, the Customer (Controller) and CleanDupTool (Processor) agree to the terms below. A counter-signed PDF copy is available on request from dpa@cleanduptool.com.

1. Definitions

"Controller", "Processor", "Personal Data", "Processing", "Data Subject" and "Supervisory Authority" have the meanings given in the UK GDPR and EU GDPR (Regulation 2016/679). "Customer Data" means CRM records (contacts, accounts, leads) the Customer uploads, imports or syncs into CleanDupTool. "Sub-processor" means any third party engaged by the Processor to process Customer Data.

2. Roles and scope

The Customer is the Controller of Customer Data. CleanDupTool is the Processor and processes Customer Data **only on documented instructions** from the Customer, which are: (a) the Terms of Service, (b) the configuration choices made in-app, and (c) any written instructions sent to dpa@cleanduptool.com.

3. Subject matter, duration, nature and purpose (Art. 28(3))

- **Subject matter:** duplicate detection, merging and cleansing of CRM records.
- **Duration:** the term of the Customer's CleanDupTool subscription, plus a 30-day return/deletion window.
- **Nature and purpose:** automated similarity matching across CRM fields, generation of merge proposals, application of approved merges back to the source CRM.
- **Categories of Data Subjects:** the Customer's prospects, customers, business contacts and employees recorded in the CRM.
- **Categories of Personal Data:** business contact details (name, email, phone, job title, employer), CRM activity metadata, and any other contact-record fields the Customer chooses to import.
- **Special category data:** not required, not requested. The Customer agrees not to upload Article 9 special-category data or criminal-conviction data.

4. Processor obligations

CleanDupTool shall:

- process Customer Data only on the Customer's documented instructions, including transfers, unless required by law (in which case CleanDupTool will notify the Customer first, where legally permitted);
- ensure persons authorised to process Customer Data are bound by confidentiality;
- implement the technical and organisational measures described in Annex 2;
- not engage a new sub-processor without complying with section 6;
- assist the Customer, taking into account the nature of processing, in responding to Data Subject requests (section 7) and in meeting its Art. 32–36 obligations (security, breach notification, DPIAs);
- at the Customer's choice, delete or return all Customer Data at the end of the subscription, unless retention is required by law;

- make available all information necessary to demonstrate compliance with Art. 28, and allow for audits as described in section 9.

5. Customer obligations

- The Customer warrants it has a valid lawful basis for processing Customer Data and for instructing CleanDupTool to process it.
- The Customer is responsible for the accuracy, legality and content of Customer Data.
- The Customer will not instruct CleanDupTool to process Customer Data in breach of Data Protection Law.

6. Sub-processors

The Customer provides a general written authorisation for CleanDupTool to engage sub-processors. The current list is in Annex 3. CleanDupTool will notify the Customer at least **30 days** before adding or replacing a sub-processor (by email to the account admin and via the website). The Customer may object on reasonable data-protection grounds within that window; if the objection cannot be resolved, the Customer may terminate the affected service for a pro-rata refund.

CleanDupTool imposes data-protection obligations on each sub-processor that are no less protective than those in this DPA, and remains fully liable for their performance.

7. Data Subject rights

Taking into account the nature of the processing, CleanDupTool will assist the Customer by appropriate technical and organisational measures, insofar as possible, to fulfil the Customer's obligation to respond to Data Subject requests (access, rectification, erasure, restriction, portability, objection). Where a request is made directly to CleanDupTool, CleanDupTool will, without undue delay, forward it to the Customer and will not respond directly except on the Customer's instructions or where legally required.

8. Personal data breach notification

CleanDupTool will notify the Customer **without undue delay and in any event within 48 hours** after becoming aware of a Personal Data Breach affecting Customer Data, providing the information required under Art. 33(3) to the extent then known, and updates as the investigation progresses.

9. Audits

CleanDupTool will make available to the Customer, on written request and subject to confidentiality, its most recent third-party security attestations and a written response to a reasonable security questionnaire, no more than once per 12-month period. Where the Customer reasonably demonstrates this is insufficient, the Customer (or a mutually agreed independent auditor, bound by confidentiality) may carry out an audit at the Customer's cost, on at least 30 days' written notice, during business hours, without disrupting CleanDupTool's operations or other customers' data.

10. International data transfers

Customer Data is hosted in the European Union. Where Customer Data is transferred to a sub-processor outside the UK / EEA in a country without a UK or EU adequacy decision, the transfer is covered by the **EU Standard Contractual Clauses (2021/914), Module 2** (Controller-to-Processor), and the UK International Data Transfer Addendum (IDTA), incorporated by reference. Docking clause applies; the parties select the optional Clause 7. Annexes I, II and III of the SCCs are populated by Annexes 1–3 of this

DPA.

11. Return and deletion

Within 30 days of termination, the Customer may export all Customer Data via the in-app export. After that window, CleanDupTool will delete Customer Data from production systems within 30 days and from encrypted backups within a further 35 days, unless retention is required by law. Anonymous, non-identifying analytics retained under our Privacy Policy are out of scope.

12. Liability and term

Each party's liability under this DPA is subject to the limitations of liability in the Terms of Service. This DPA takes effect on the earlier of (a) the Customer's acceptance of the Terms of Service, or (b) the first upload of Customer Data, and remains in force for as long as CleanDupTool processes Customer Data.

Annex 1 — Processing details

- **Processing operations:** ingest, normalise, fingerprint, match (exact + fuzzy + AI), present merge proposals, apply approved merges to source CRM, export results.
- **Frequency:** continuous during subscription term.
- **Retention:** Customer Data is retained for the subscription term and deleted per section 11.
- **Recipients:** the Customer's authorised users and the sub-processors listed in Annex 3.

Annex 2 — Technical and organisational measures (Art. 32)

- **Encryption:** TLS 1.2+ in transit; AES-256 at rest for the primary database and backups.
- **Access control:** least-privilege Row-Level Security at the database layer; role-based access in app; SSO/MFA for staff admin access; no shared production accounts.
- **Tenant isolation:** per-organisation segregation enforced by RLS policies on every Customer Data table.
- **Network:** private networking between application and database; no direct public database access.
- **Backups:** automated daily backups, encrypted, retained 35 days, integrity-tested.
- **Logging & monitoring:** audit log of admin actions and merges; alerting on anomalous activity.
- **Vulnerability management:** dependency scanning, automated security advisories, scheduled patching.
- **Secure development:** code review on every change, automated tests, principle of least privilege in service accounts.
- **Personnel:** confidentiality obligations for all staff; security awareness training; background checks for staff with production access where lawful.
- **Incident response:** documented runbook, on-call rotation, 48-hour breach notification (section 8).
- **Sub-processor due diligence:** contractual data-protection terms equivalent to this DPA.
- **Business continuity:** infrastructure on multi-AZ managed services; recovery objectives reviewed annually.

Annex 3 — Sub-processors

The following sub-processors are engaged to deliver the CleanDupTool service. The Customer is notified of changes per section 6.

Sub-processor	Purpose	Location
Supabase	Database, authentication, file storage	EU (eu-west)
Cloudflare	Edge hosting, CDN, DDoS protection	Global edge; EU-resident origin
Stripe Payments Europe	Billing and subscription management (no CRM data)	EU / US (SCCs)
Resend / email provider	Transactional email (account & billing only)	EU / US (SCCs)

The legal entity name, registered country and signatory details will be added here once finalised. For a counter-signed PDF version, email dpa@cleanduptool.com.