Data Processing Agreement

Pursuant to Art. 28(3) GDPR

This Data Processing Agreement (“DPA”) forms part of the Tulu Terms of Service. By creating a Tulu account, clicking ‘I Agree’ during the registration or checkout process, or otherwise using the Tulu Software, the customer (the “Client”) electronically executes and agrees to be bound by this DPA. The Client’s details, including name and contact information, are determined by the billing and account information provided during the Tulu registration process.

Preamble

The Client commissions Tulu GmbH (the “Contractor”) to process data within the scope of a software service. The Contractor provides services to the Client in the field of digital marketing, in particular for the visualization and analysis of CRM data. In doing so, personal data of the

Client's customers may be processed. This agreement specifies the data protection obligations under Art. 28 GDPR.

1. **Subject matter and duration of the contract**
   a. The subject matter of this agreement is the modalities of order processing and subcontracting by the Contractor.
   b. The Client wishes to use the Contractor's software services to optimise its customer relationships and make its marketing measures as efficient as possible. In the course of providing its contractually agreed services, the Contractor must process data, in particular marketing data, belonging to the Client. Under certain circumstances, this data may also contain personal data belonging to the Client's customers.
   c. The Contractor shall provide the software services described in accordance with the provisions of the GDPR, in particular Art. 28 GDPR.
   d. The effectiveness and term of this agreement are governed by the software service agreement between the parties.
   e. Insofar as other agreements between the Client and the Contractor result in other arrangements for the protection of personal data, this agreement on order processing shall take precedence, unless the parties expressly agree otherwise.

2. **Processing of personal data**
   a. The Client may itself be the controller or processor with regard to the data. The Contractor shall accordingly act as a processor or sub-processor.
   b. The Contractor shall treat the data provided to it by the Client as confidential. The Contractor shall also ensure that its employees are trained in the handling of confidential information.
   c. **Subject of the processing.** The data of the Client's customers may include the following types of data, which do not necessarily have to be personal data:

- First and last names
- Email address
- Company name
- Address of the place of business
- IP address
- Device and browser type
- Operating system
- Time and duration of use

3. **Technical and organizational measures**
   a. The Contractor shall take all necessary technical and organizational measures within its area of responsibility in accordance with Art. 32 GDPR to protect personal data, and shall provide the Client with the documentation for review upon request. If the review reveals a need for adjustment, this shall be implemented by mutual agreement.
   b. The agreed technical and organizational measures are subject to technical progress and further development. In this respect, the Contractor shall be permitted to implement alternative adequate measures in the future. In doing so, the security level of the specified measures must not be compromised. The Client shall be informed immediately of any significant changes, which shall be documented by the Contractor.

4. **Rights of data subjects**
   a. The Contractor shall support the Client in its area of responsibility and, as far as possible, by means of suitable technical and organizational measures in responding to and implementing requests from data subjects regarding their data protection rights. It may not disclose, transfer, correct, delete, or restrict the processing of data processed on behalf of the Client, except on the Client's own authority and only in accordance with the Client's documented instructions.

b. If a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.
c. Insofar as this is covered by the scope of services, the rights to information, correction, restriction of processing, deletion, and data portability shall be ensured directly by the Contractor in accordance with the documented instructions of the Client.

5. **Quality assurance and other obligations of the contractor**
   a. In addition to complying with the provisions of this contract, the Contractor has its own legal obligations under the GDPR; in this respect, it shall in particular ensure compliance with the following requirements:
      - **Maintaining confidentiality** in accordance with Art. 28(3)(2)(b), 29, 32(4) GDPR: When carrying out the work, the Contractor shall only employ staff who are bound to confidentiality and have been familiarised in advance with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who has legitimate access to personal data may only process this data in accordance with the Client's instructions, including the powers granted in this contract, unless they are legally obliged to process it.
      - The Client and the Contractor shall cooperate with the supervisory authority in the performance of its tasks upon request.
      - The Client shall be informed without delay of any control activities and measures taken by the supervisory authority insofar as they relate to this contract. This shall also apply if a competent authority investigates the Contractor in the context of administrative or criminal proceedings relating to the processing of personal data during order processing.
      - If the Client is subject to an inspection by the supervisory authority, administrative offense, or criminal proceedings, a liability claim by a data subject or a third party, another claim,

or a request for information in connection with the processing of orders by the Contractor, the Contractor shall support the Client to the best of its ability.

- The Contractor shall regularly monitor internal processes and technical and organizational measures to ensure that processing within its area of responsibility is carried out in accordance with the requirements of applicable data protection law and that the rights of the data subject are protected.
- Verifiability of the technical and organizational measures taken vis-à-vis the Client within the scope of its control powers under Annex 1 of this contract.
- The Contractor shall immediately report any breaches of personal data protection to the Client in such a way that the Client can fulfill its legal obligations, in particular under Articles 33 and 34 of the GDPR. The Contractor shall prepare documentation on the entire process and make it available to the Client for further action.
- The Contractor shall support the Client in its area of responsibility and, insofar as possible, within the scope of existing information obligations to supervisory authorities and data subjects, and shall provide the Client with all relevant information without delay.
- If the Client is obliged to carry out a data protection impact assessment, the Contractor shall support the Client, taking into account the nature of the processing and the information available to it. The same applies to any existing obligation to consult the competent data protection supervisory authority.

b. This contract does not release the Contractor from compliance with other provisions of the GDPR.

6. **Reporting of security incidents**

a. If the Contractor notices a security breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorised

disclosure of, or access to, personal data of customers or other data during processing by the Contractor (in each case a "security incident"), the Contractor shall immediately and without undue delay (1) notify the Client of the security incident; (2) investigate the security incident and provide the Client with detailed information about the security incident; (3) take appropriate measures to mitigate the impact and minimise the damage resulting from the security incident.

b. Notifications of security incidents shall be sent to the Client in the manner chosen by the Contractor, for example by email to the primary email address associated with the Client's Tulu account. It is the Client's sole responsibility to ensure the Contractor has the correct contact information for the Client. The Client is solely responsible for complying with its obligations under applicable law to report such incidents and to fulfill reporting obligations to third parties regarding security incidents.
c. The Contractor shall use reasonable efforts to assist the Client in fulfilling its obligation under Article 33 of the GDPR or other applicable laws or regulations to notify the competent supervisory authority and the data subjects of such security incidents.
d. The reporting of a security incident or the response to a security incident by the Contractor in accordance with this section does not imply that the Contractor acknowledges any fault or liability in relation to the security incident in question.

7. **Subcontracting**
   a. Subcontracting relationships within the meaning of this provision are understood to be those services that are directly related to the provision of the main service. This does not include ancillary services used by the Contractor, e.g. telecommunications services, postal/transport services, cleaning services or security services. Maintenance and testing services constitute a subcontracting relationship if they are provided for IT systems in

connection with a service provided by the Contractor under this contract.

b. However, the Contractor is obliged to enter into appropriate and legally compliant contractual agreements and to take control measures to ensure the data protection and data security of the Client's data, even in the case of outsourced ancillary services.
c. The Contractor may only commission subcontractors (additional processors) with the prior express written or documented consent of the Client, unless they were already commissioned when the main contract was concluded. Existing contractors must be disclosed in a separate document.
d. Outsourcing to subcontractors or changing existing subcontractors is permitted:
   - provided that the Contractor notifies the Client of such outsourcing to subcontractors in advance in writing or in text form within a reasonable period of time, which may not be less than 14 days, and
   - the Client does not object to the planned outsourcing in writing or in text form to the Contractor by the time the data is handed over, and
   - a contractual agreement in accordance with Art. 28(2-4) GDPR serves as the basis.
e. The transfer of the Client's personal data to the subcontractor and the subcontractor's initial activities are only permitted once all the requirements for subcontracting have been met. Compliance with and implementation of the technical and organizational measures at the subcontractor's premises shall be checked in advance of the processing of personal data and then regularly by the Contractor, taking into account the risk at the subcontractor's premises. The Contractor shall provide the Client with the results of the checks upon request. The Contractor shall also ensure that the Client can exercise its rights under this agreement (in particular its rights of control) directly against the subcontractors.

f. If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure compliance with data protection law by taking appropriate measures. The same applies if service providers within the meaning of paragraph 1, sentence 2 are to be used.
g. Any further outsourcing by the subcontractor requires the express written consent of the main Contractor. All contractual provisions in the contract chain shall also be imposed on the further subcontractor.

8. **International data transfers**
   a. Any transfer of personal data to a third country or to an international organization requires compliance with the provisions on the transfer of personal data to third countries in Chapter V of the GDPR.
   b. The Client permits data transfers to a third country to the subcontractors disclosed by the Contractor in accordance with Section 7. The Contractor is responsible to the Client for ensuring an adequate level of protection in accordance with Art. 44 ff. GDPR within the scope of subcontracting.
   c. If the Client instructs the transfer of data to third parties in a third country, it shall be responsible for compliance with Art. 44 ff. GDPR.

9. **Client's rights of control**
   a. The Client has the right, in consultation with the Contractor, to carry out checks or have them carried out by auditors to be appointed in individual cases. The Client has the right to verify the Contractor's compliance with this agreement in its business operations during normal business hours by means of random checks, which must generally be announced in good time.
   b. The Contractor shall ensure that the Client can verify the Contractor's compliance with its obligations under Art. 28 GDPR. The Contractor undertakes to provide the Client with the

necessary information upon request and, in particular, to provide evidence of the implementation of technical and organizational measures.

10. **Authority of the client to issue instructions**
    a. The Contractor shall only process personal data on the basis of documented instructions from the Client, unless it is obliged to do so under the law of the Member State or under Union law. The Client shall confirm verbal instructions immediately (at least in text form). The Client's initial instructions are set out in this contract.
    b. The Contractor shall inform the Client immediately if it believes that an instruction violates data protection regulations. The Contractor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client.

11. **Deletion and return of personal data**
    a. Copies or duplicates of the data shall not be made without the Client's knowledge. This does not apply to backup copies insofar as they are necessary to ensure proper data processing, or to data necessary to comply with statutory retention obligations.
    b. Upon completion of the contractually agreed work or earlier upon request by the Client – but no later than upon termination of the service agreement – the Contractor shall hand over to the Client all documents that have come into its possession, processing and usage results created, and data stocks related to the contractual relationship, or destroy them in accordance with data protection regulations after prior consent. The same applies to test and reject material. The deletion log must be presented upon request.

12. **Miscellaneous**
    a. The liability of the parties under this agreement is subject to the limitations of liability in the main contract.

b. This agreement is not a separate agreement and is therefore only valid for as long as the main contract is in force. Verbal side agreements are not valid. The headings in this agreement are for clarity only and should not be used to interpret the clauses.
c. Should any provision of this agreement be invalid, the validity of the remainder of the agreement shall not be affected. The invalid provision shall be replaced by the statutory provision.
d. Amendments or additions to this agreement shall only be effective if they are agreed in writing by the parties. Amendments to the written form requirement must also be agreed in writing.
e. This agreement is subject to German law. The place of jurisdiction for all disputes arising from or in connection with this agreement is Munich.
f. This agreement shall be valid even without a signature, provided that the main contract has been validly concluded. If the Client requires a signed version of this agreement, the Contractor may provide a signed version to the Client.

Annex 1 — Technical and Organisational Measures (TOMs)

Data Protection Documentation prepared pursuant to Article 32 GDPR

Tulu GmbH · Stollbergstr. 22, 80539 Munich · adrian@tulu.tech · alltulu.com

1. Confidentiality

1.1 Physical Access Control

Controls preventing unauthorised persons from accessing systems that process personal data.

Technical Measures

- Physical infrastructure hosted on Google Cloud Platform (GCP); physical access controls are entirely managed by Google and certified to ISO 27001 and SOC 2 Type II.
- Automatic screen lock enabled on all workstations (company policy).
- Company workstations use full-disk encryption (FileVault).

Organisational Measures

- Employees working in secure office space — keycard and security officer (hybrid model) are instructed to lock screens when stepping away from their workstation.
- Employees avoid working with customer data on screens visible to others in shared/public spaces.
- No printed documents containing customer personal data are produced.
- Visitors to company premises are accompanied by employees at all times.

Additional Measures: Physical server infrastructure is managed exclusively by Google Cloud Platform. No on-premises servers are operated by Tulu GmbH. Work space access is secured via access control systems (chip-card entry and security guard). Company personnel follow a clean-desk and screen-lock policy at all shared office locations.

1.2 System Access Control

Measures preventing unauthorised use of data processing systems.

Technical Measures

- Multi-factor authentication (MFA) enforced on: GCP Console, BigQuery, Google Workspace (company email), and GitHub (code repository).
- Login to all production systems requires username and password plus MFA second factor.
- Built-in malware protection active on all company workstations.
- GCP firewall rules restrict access to production infrastructure by IP and service account.
- Encryption of all company-issued workstations via FileVault.
- External USB interface access restricted by company hardware system settings.

Organisational Measures

- User permissions for production systems managed centrally; access granted on a need-to-know basis.
- Secure password policy enforced: minimum length, complexity, no password reuse.
- Mobile device policy in place for all company-issued devices.
- Clean desk policy observed at company working locations.
- Manual desktop lock instruction issued to all staff.
- General data protection policy shared with all team members.

Additional Measures: All production access requires MFA without exception. Hard drive encryption is enforced via FileVault across all company devices. Endpoint malware protection is provided by Apple XProtect (updated automatically with company hardware security updates).

1.3 Data Access Control

Measures ensuring authorised users can only access data within their access scope, and that data cannot be read, copied, modified, or removed without authorisation.

Technical Measures

- Access to production data in BigQuery is restricted to a maximum of two (2) senior engineering leads.
- BigQuery Data Access Logs: logging of all queries, access events, and data modifications will be activated. [Action item: enable Cloud Audit Logs > Data Access in GCP Console]
- Role-based access control (RBAC) enforced via GCP IAM; permissions scoped to minimum required for each role.
- Physical deletion of data on device decommissioning (secure wipe).

Organisational Measures

Production data access is limited to the two most senior engineering leads. All access changes are handled immediately upon any personnel change. GCP IAM is used to enforce and document all permission assignments.

- Access to production customer data is granted on a strict need-to-know basis.
- Minimum number of administrators — maximum two (2) individuals hold production data access.
- Upon change in personnel (including termination or role change), access rights to all production systems are revoked immediately.
- Authorization concept maintained and reviewed upon any personnel change.
- Internal data protection responsible: Dahvid Simcha NessAiver, Engineering Team Lead.

Additional Measures: Production data access is limited to the two most senior engineering leads. All access changes are handled immediately upon any personnel change. GCP IAM is used to enforce and document all permission assignments.

1.4 Separation Control

Measures ensuring that data collected for different purposes can be processed separately.

Technical Measures

- Each customer's data is stored in a logically separate BigQuery dataset, identified by a unique customer identifier.
- No cross-customer data access is possible; GCP IAM policies enforce dataset-level isolation.
- Production and development/test environments are maintained as separate GCP projects.
- No customer can access another customer's data through the application.

Organisational Measures

- Authorization concept controls dataset-level access per customer.
- Database rights defined and enforced at the BigQuery dataset level.
- Data records are tagged with purpose and customer attributes.
- Test environments use anonymised or synthetic data only — no production customer data is used in testing.

Additional Measures: Customer data separation is enforced architecturally via separate BigQuery datasets per customer. This ensures that even in the event of an application-layer error, cross-customer data exposure is prevented at the infrastructure level.

1.5 Pseudonymisation

Processing of personal data so that it can no longer be attributed to a specific data subject without the use of additional information held separately.

Technical Measures

- All personally identifiable information (PII) is stripped from data before ingestion into BigQuery. No PII is stored in the production data warehouse.
- Internal debugging, testing, and analysis is performed exclusively on anonymised or synthetic data. Real customer PII is never used in a non-production context.
- Data flowing from external sources (HubSpot API, CSV uploads) is processed through a stripping pipeline before storage.

Organisational Measures

- Internal instruction issued to all engineering staff: personal data must be anonymised or pseudonymised before any internal processing, debugging, or disclosure.
- Re-identification of stripped data is not performed except where strictly required for customer support, under controlled access.

Additional Measures: Tulu's architecture implements pseudonymisation as a foundational design principle: the production BigQuery data warehouse contains no PII. Only aggregated marketing metrics and revenue data (stripped of all individual identifiers) are stored. User account data (names and emails) is held separately in the application user management layer with its own access controls.

2. Integrity

2.1 Transfer Control

Measures ensuring that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport.

Tulu GmbH operates three data transfer flow types, covering all sub-processors:

Flow A — Manual CSV Ingestion (Gmail → Firebase → BigQuery): Customers send CSV files containing marketing or revenue data to a designated Gmail inbox. An automated Firebase Cloud Function is triggered upon receipt, which processes and uploads the file to BigQuery over an encrypted HTTPS connection. All PII is stripped before data is written to BigQuery. The raw CSV file is never stored in BigQuery. The source email and attachment reside only in Google Workspace Gmail and are automatically purged after 30 days. The Firebase function retains no copy of the raw file.

Flow B — OAuth API Integrations (Scheduled Data Ingestion): This flow covers all connected ad and analytics platforms, as well as CRM integrations: HubSpot, Google Ads, LinkedIn Ads, Reddit Ads, Microsoft/Bing Ads, Meta/Facebook Ads, Matomo Analytics, and Google Analytics (GA4). Upon initial customer authorisation via OAuth 2.0, a one-time connection is established per platform. All subsequent data syncs are performed on an automated schedule. Data is transmitted from each platform's API to Tulu's infrastructure over encrypted HTTPS connections. All data is stripped of PII before ingestion into BigQuery. Only aggregated marketing metrics, campaign performance data, and

site analytics figures are stored. No personal data is transmitted or stored at any point in this flow.

Flow C — LLM Processing via Anthropic API (Outbound): Aggregated, anonymised data (with all PII stripped prior to transmission) is sent outbound to the Anthropic API for processing and analysis. This flow is outbound rather than inbound — Tulu's systems initiate the transfer to Anthropic. No personal data is transmitted to Anthropic at any stage. All communication occurs over encrypted HTTPS connections.

Technical Measures

- All data transmission between Tulu and sub-processors uses encrypted connections (HTTPS/TLS 1.2+).
- Flow A: Firebase Cloud Functions process CSV ingestion over encrypted channels only.
- Flow B: All OAuth API integrations (HubSpot, Google Ads, LinkedIn Ads, Reddit Ads, Bing Ads, Meta Ads, Matomo, Google Analytics) use OAuth 2.0 authorisation and HTTPS for all data transfer.
- Flow C: Anthropic API communication uses HTTPS/TLS encryption.
- BigQuery data at rest is encrypted by default using Google-managed encryption keys.
- Gmail (Google Workspace) provides TLS encryption for incoming email.

Organisational Measures

- Raw CSV files are not retained beyond the Gmail 30-day automatic purge cycle.
- PII stripping is performed programmatically at the point of ingestion across all three flow types before any data reaches BigQuery.
- Documentation of all data transfer flows maintained internally and reflected in the sub-processor register.
- Customers are informed of all connected integrations and data ingestion methods at onboarding and via the DPA.

- Sub-processor agreements in place with all platforms listed in Annex 2.

Additional Measures: All data flows are encrypted in transit. PII is stripped at the point of ingestion. No raw customer files containing PII are stored in Tulu's data warehouse infrastructure.

2.2 Input Control

Measures ensuring it is possible to check and determine whether and by whom personal data has been entered, modified, or deleted in data processing systems.

Technical Measures

- BigQuery job history provides automatic logging of all query execution, data insertion, modification, and deletion events, including the identity of the executing service account or user.
- Firebase Cloud Function logs record each execution of the CSV ingestion pipeline, including timestamp and processing outcome.
- GCP Cloud Audit Logs record administrative actions on all production infrastructure.
- BigQuery Data Access Logs: Enabled.

Organisational Measures

- All data entry, modification, and deletion in BigQuery is attributable to individual authenticated identities (not shared accounts or groups).
- Rights to write, modify, or delete data are assigned based on the authorization concept; only the two designated engineering leads hold write access.
- Clear responsibilities for data deletion are defined and documented.
- Log retention period follows GCP default (400 days for Audit Logs).

Additional Measures: BigQuery's built-in job history provides a complete audit trail of all data operations. Firebase Cloud Functions provide execution logs for all automated ingestion jobs. These logs are retained in GCP and accessible for review.

3. Availability and Resilience

3.1 Availability Control

Measures ensuring personal data is protected against accidental destruction or loss.

Technical Measures

- BigQuery data is stored on Google Cloud Platform, which provides multi-zone redundancy and automatic data replication.
- BigQuery provides built-in table recovery for up to 7 days following accidental deletion (table snapshots / time travel).
- BigQuery dataset-level snapshots available for point-in-time recovery.
- GCP infrastructure provides 99.99% uptime SLA for BigQuery.
- All application services (Firebase Functions) run on GCP managed infrastructure with automatic failover.

Organisational Measures

- Recovery plan documented: in the event of data loss, data can be re-pulled from all connected source systems (HubSpot API, CSV re-upload) covering the preceding 6 months. If required, a manual re-ingestion process can be triggered for a longer historical period.
- Backup and recovery capability is monitored and tested periodically.
- GCP status alerts are monitored to detect infrastructure incidents promptly.

- Storage of critical configuration and ingestion logic in version-controlled repository (GitHub) ensures recoverability of application code.

Additional Measures: Infrastructure availability is primarily managed by Google Cloud Platform. Tulu GmbH maintains a documented data recovery procedure based on re-ingestion from connected source systems. BigQuery's native time-travel feature (7-day table recovery) provides an additional safety net for accidental deletion events.

4. Procedures for Regular Review, Assessment, and Evaluation

4.1 Data Protection Measures

Technical Measures

- GCP Cloud Audit Logs provide centralised documentation and monitoring of all data processing activities.
- Automated daily log reports surface security issues and anomalies for review.
- BigQuery Data Access Logs: Enabled.
- Internal documentation of data processing procedures and data flows maintained.
- A review of the effectiveness of technical protective measures is carried out at least once per year.

Organisational Measures

- Internal Data Protection Responsible: Dahvid Simcha NessAiver, Engineering Team Lead (dahvid@tulu.tech).

- All employees have received data protection awareness training. Training is conducted on an ongoing basis whenever new developments, risks, or regulatory changes arise.
- All employees handling personal data are committed to confidentiality.
- Data Processing Agreements (DPAs) are in place with all customers (Tulu acts as data processor).
- Data protection impact assessments (DPIAs) are conducted as required.
- The organisation complies with information obligations under Articles 13 and 14 of the GDPR.
- A formalised process for handling data subject requests (access, erasure, portability) is in place.

Additional Measures: Data protection responsibility is owned by the Engineering Team Lead. Awareness training is provided on an ongoing ad-hoc basis in response to new information, regulatory updates, or internal incidents. Annual formal review of all technical and organisational measures is conducted.

4.2 Incident Response Management

Support in responding to security breaches.

Technical Measures

- Automated daily log reporting: GCP Cloud Audit Logs and application logs are reviewed via automated daily reports that surface anomalies and potential security issues.
- GCP Security Command Center alerts configured for unusual access patterns.
- Firewall rules and GCP VPC security controls actively in place.

- Firebase Function execution logs monitored for anomalous pipeline behaviour.

Organisational Measures

- Documented incident response escalation chain: (1) Engineering Team Lead (Dahvid Simcha NessAiver) is notified immediately upon detection; (2) C-Suite executives are informed; (3) affected customer(s) are notified without undue delay.
- In the event of a personal data breach, the competent supervisory authority (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI — Germany) is notified within 72 hours of becoming aware of the breach, in accordance with Article 33 GDPR.
- Affected data subjects are notified without undue delay where the breach is likely to result in high risk, in accordance with Article 34 GDPR.
- Security incidents and data breaches are documented internally (incident log).
- Post-incident review is conducted to implement corrective measures and prevent recurrence.

Additional Measures: Incident detection is supported by automated daily log reporting. The 72-hour reporting obligation under Article 33 GDPR is acknowledged and built into the incident response escalation procedure.

4.3 Privacy by Design / Privacy by Default

Technical Measures

- Only the minimum personal data necessary for the respective processing purpose is collected. User account data is limited to name and email address.
- PII is stripped at the point of ingestion into the data warehouse — no personal data enters BigQuery.

- Raw CSV files containing customer data are not stored beyond the 30-day automatic Gmail purge cycle.
- Internal development and testing is performed exclusively with anonymised or synthetic data.
- LLM processing (Anthropic API) is performed only on anonymised, aggregated data with no PII.
- Easy exercise of data subject rights is supported by the application architecture.

Organisational Measures

- Data minimisation is a foundational architectural principle: no more data is collected than is strictly necessary.
- Privacy-by-design is considered at every stage of feature development.
- Default settings favour privacy: data sharing is opt-in, not opt-out.
- Customers are informed at onboarding of the data they are sharing and how it is used.

Additional Measures: The decision not to store raw CSV files, the PII stripping pipeline, and the exclusive use of anonymised data for internal processing all represent concrete implementations of the privacy-by-design and privacy-by-default principles under Article 25 GDPR.

4.4 Processor Obligations

Measures ensuring that personal data processed on behalf of clients is handled only in accordance with client instructions.

- Data Processing Agreements (DPAs) are in place with all customers. Tulu GmbH acts as data processor; the customer is the data controller.
- Selection of sub-processors is based on due diligence with regard to data protection and security.

- Written processing instructions are documented in the DPA with each customer.
- Employees are obligated to maintain data confidentiality.
- Effective control rights vis-à-vis sub-processors are agreed contractually.
- Sub-processor obligations are flowed down to all third-party providers.
- Destruction of customer data upon contract termination is ensured and documented.
- For longer-term customer relationships, ongoing review of sub-processor protection levels is conducted.

Annex 2 — Authorised Sub-processors

Google Cloud Platform (GCP) / BigQuery
Purpose: Cloud infrastructure, data warehouse, storage.
Legal basis: Google Cloud DPA — accepted via GCP Terms of Service (covers GDPR Article 28).

Google Workspace / Gmail
Purpose: Incoming customer CSV file receipt; automatic 30-day purge.
Legal basis: Google Workspace DPA — accepted via Google Workspace Terms of Service.

HubSpot
Purpose: CRM data integration via API.
Legal basis: HubSpot Data Processing Agreement in place.

Anthropic (Claude API)
Purpose: LLM processing of anonymised, aggregated data only (no PII transmitted).
Legal basis: Art. 28 GDPR / Standard Contractual Clauses (SCCs).

Google Ads API
Purpose: Marketing campaign metrics ingestion (no PII). OAuth-triggered connection, then scheduled API pull.
Legal basis: Google Ads API Terms of Service including Google GDPR Data Processing Addendum.

LinkedIn Ads API
Purpose: Marketing campaign metrics ingestion (no PII). OAuth-triggered connection, then scheduled API pull.
Legal basis: LinkedIn API Terms of Service including LinkedIn Data Processing Agreement.

Reddit Ads API
Purpose: Marketing campaign metrics ingestion (no PII). OAuth-triggered connection, then scheduled API pull.
Legal basis: Reddit Ads API Terms of Service including Reddit Data Processing Agreement.

Microsoft / Bing Ads API
Purpose: Marketing campaign metrics ingestion (no PII). OAuth-triggered connection, then scheduled API pull.
Legal basis: Microsoft Advertising API Terms of Service including Microsoft GDPR Data Processing Addendum.

Meta / Facebook Ads API
Purpose: Marketing campaign metrics ingestion (no PII). OAuth-triggered connection, then scheduled API pull.
Legal basis: Meta Business Tools Terms including Meta Data Processing Terms (GDPR).

Matomo Analytics API
Purpose: Site analytics data ingestion (no PII). OAuth-triggered connection, then scheduled API pull.
Legal basis: Matomo Data Processing Agreement (self-hosted or cloud, as applicable per customer deployment).

Google Analytics API (GA4)
Purpose: Site analytics data ingestion (no PII). OAuth-triggered connection, then scheduled API pull.
Legal basis: Google Analytics DPA — accepted via Google Measurement Controller-Controller Data Protection Terms.

Additional Measures: All sub-processors listed above are subject to contractual data processing obligations. Sub-processor selection is based on due diligence regarding data protection compliance and security certifications. No sub-processors outside the above list are used for processing customer personal data.

This DPA forms part of the Tulu Terms of Service.