CORGENT

by Malango Tech

Data Processing Agreement

GDPR Article 28 · Auftragsverarbeitungsvertrag (AVV)

This Data Processing Agreement governs the Processing of Personal Data by Malango Tech UG (haftungsbeschränkt) i.G., trading as “Corgent”, when acting as a Processor on behalf of the Customer in connection with the Corgent AI agent platform and related services. It incorporates the EU Standard Contractual Clauses and addresses UK and Swiss transfers.

Document	Data Processing Agreement (DPA / AVV)
Version	1.0
Effective date	24 June 2026
Processor	Malango Tech UG (haftungsbeschränkt) i.G. — “Corgent”
Registered address	Schumannstraße 24, 71640 Ludwigsburg, Germany
Data protection contact	mk@corgent.ai
Governing law	Federal Republic of Germany

Contents

Background

This Data Processing Agreement, including its Annexes (the **“DPA”** or **“AVV”**), forms part of and is incorporated into the agreement between the Customer and Corgent for the provision of the Services (the **“Principal Agreement”**). It records the Parties’ agreement with regard to the Processing of Customer Personal Data and is concluded pursuant to Article 28(3) of Regulation (EU) 2016/679 (the **“GDPR”**) and other Applicable Data Protection Laws.

Where the Customer acts as a controller and Corgent acts as a processor in respect of Customer Personal Data, this DPA applies. Where the Customer is itself a processor acting on behalf of a third-party controller, Corgent acts as a sub-processor and this DPA applies *mutatis mutandis* . In the event of any conflict between this DPA and the Principal Agreement on the subject matter of data protection, this DPA prevails; in the event of any conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses prevail.

The Parties

Processor: Malango Tech UG (haftungsbeschränkt) i.G., trading as “Corgent”, Schumannstraße 24, 71640 Ludwigsburg, Germany, represented by its managing director Maximilian Koch (“ **Corgent** ”, the “ **Processor** ”).

Customer: The legal entity or person that has entered into the Principal Agreement with Corgent and that acts as controller (or processor) in respect of Customer Personal Data (the “ **Customer** ”, the “ **Controller** ”).

Together: The Customer and Corgent are each a “ **Party** ” and together the “ **Parties** ”.

Company status: company in formation (i.G.). Commercial register entry has been applied for at the Local Court of Stuttgart (Amtsgericht Stuttgart); the commercial register number will be added after registration. The VAT identification number has been applied for with the Federal Central Tax Office and will be added once issued. Personal liability of the acting persons applies until registration.

1. Definitions and Interpretation

1.1 Capitalised terms used but not defined in this DPA have the meaning given to them in the Principal Agreement. The following definitions apply to this DPA:

- **“Applicable Data Protection Laws”** means all laws and regulations applicable to the Processing of Personal Data under this DPA, including the GDPR; the German Federal Data Protection Act (BDSG); the UK GDPR and the UK Data Protection Act 2018 (the **“UK Data Protection Laws”**); the Swiss Federal Act on Data Protection (the **“Swiss FADP”**); and, to the extent applicable, U.S. State Privacy Laws.
- **“Controller”** , **“Processor”** , **“Data Subject”** , **“Personal Data”** , **“Processing”** , **“Personal Data Breach”** and **“Supervisory Authority”** have the meanings given in Article 4 of the GDPR (or the equivalent terms, such as “business” and “service provider”, under other Applicable Data Protection Laws).
- **“Customer Personal Data”** means any Personal Data that Corgent Processes on behalf of the Customer in the course of providing the Services, as further described in Annex I.
- **“Services”** means the Corgent AI agent platform and related products made available under the Principal Agreement, including the discovery, deployment, configuration and execution of AI agents, the manager chat experience, customer-activated integrations, and associated APIs.
- **“Standard Contractual Clauses”** or **“SCCs”** means the standard contractual clauses for the transfer of Personal Data to third countries adopted by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021, as further specified in Annex IV.
- **“UK Addendum”** means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the UK

Data Protection Act 2018, version B1.0.

- **“Subprocessor”** means any processor (including any Corgent affiliate or third party) engaged by Corgent to Process Customer Personal Data, as listed in Annex III.
- **“U.S. State Privacy Laws”** means U.S. state data protection laws in force from time to time, including the California Consumer Privacy Act as amended (the **“CCPA”**).

1.2 Headings are for convenience only and do not affect interpretation. References to a statute or statutory provision include any subordinate legislation and any amendment, re-enactment or replacement of it. The words “include”, “including” and “in particular” are without limitation.

2. Scope, Roles of the Parties and Order of Precedence

2.1 This DPA applies where, and to the extent that, Corgent Processes Customer Personal Data on behalf of the Customer in the course of providing the Services. It applies in addition to, and does not replace, any other data protection obligations of the Parties under the Principal Agreement or Applicable Data Protection Laws.

2.2 In respect of Customer Personal Data, the Customer is the Controller (or, where the Customer is itself a processor for a third-party controller, a processor) and Corgent is the Processor (or sub-processor). Each Party is responsible for complying with the obligations applicable to it under Applicable Data Protection Laws.

2.3 Corgent additionally acts as an **independent controller** in respect of certain limited data that it Processes for its own business purposes (such as account administration, billing, security, fraud prevention, and service improvement). Such Processing is described in Section 16 and is governed by the Corgent Privacy Policy rather than by the controller-to-processor terms of this DPA.

2.4 Order of precedence. In the event of any conflict or inconsistency, the following order applies, with the higher-listed document prevailing on the subject matter of data protection to the extent of the conflict: (i) the Standard Contractual Clauses (and any UK or Swiss transfer mechanism); (ii) this DPA, including its Annexes; (iii) the Principal Agreement.

3. Subject Matter and Details of the Processing

3.1 The subject matter, nature and purpose of the Processing, the types of Customer Personal Data, the categories of Data Subjects, and the duration of the Processing are described in **Annex I (Description of the Processing)** , which forms an integral part of this DPA.

3.2 Corgent shall Process Customer Personal Data only for the purposes described in Annex I and only in accordance with the Customer’s documented instructions, including with regard to transfers of Customer Personal Data to a third country, unless Corgent is required to Process such data by Union or Member State law to which it is subject. In such a case, Corgent shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

3.3 The Customer’s instructions are set out in this DPA and the Principal Agreement, and may be supplemented through the configuration choices the Customer makes within the Services (for example, the agents and integrations the Customer enables, the inputs the Customer submits, retention settings, and approval modes in the manager chat). Additional or amended instructions must be agreed in writing (which includes text form) and may be subject to adjustment of fees where they require material additional effort.

3.4 Corgent shall immediately inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Laws. Corgent may suspend execution of the relevant instruction until it is confirmed or amended by the Customer, without this constituting a breach of the

Principal Agreement.

4. Obligations of Corgent as Processor

Corgent shall:

- Process Customer Personal Data only on documented instructions from the Customer, as set out in Section 3, including with regard to international transfers;
- ensure that persons authorised to Process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and are subject to suitable access controls and training;
- implement and maintain the technical and organisational measures set out in **Annex II** in accordance with Article 32 GDPR;
- respect the conditions for engaging Subprocessors set out in Section 6;
- taking into account the nature of the Processing, assist the Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to requests from Data Subjects exercising their rights (Section 7);
- assist the Customer in ensuring compliance with the obligations under Articles 32 to 36 GDPR (security of Processing, breach notification, data protection impact assessments and prior consultation), taking into account the nature of Processing and the information available to Corgent;
- at the choice of the Customer, delete or return all Customer Personal Data after the end of the provision of the Services, and delete existing copies unless storage is required by law (Section 12); and
- make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, and allow for and contribute to audits, including inspections, as set out in Section 11.

4.1 Corgent shall not Process Customer Personal Data for its own purposes outside the scope of the Customer's instructions, and shall not sell or "share" Customer Personal Data (as those terms are defined under U.S. State Privacy Laws), nor retain, use or disclose Customer Personal Data outside the direct business relationship or for any purpose other than performing the Services.

4.2 Corgent shall maintain a record of all categories of Processing activities carried out on behalf of the Customer in accordance with Article 30(2) GDPR and shall make this record available to the Customer or a competent Supervisory Authority on request.

5. Customer Obligations and Instructions

5.1 The Customer is responsible for ensuring that it has a valid legal basis under Applicable Data Protection Laws for the Processing of Customer Personal Data and for the transmission of such data to Corgent, and that it has provided all required notices and obtained all required consents from Data Subjects.

5.2 The Customer warrants that its instructions, including the configuration of agents, integrations and inputs submitted to the Services, comply with Applicable Data Protection Laws, and that it will not use the Services to Process Personal Data in a manner that exceeds or is incompatible with the purposes described in Annex I.

5.3 Data minimisation. The Services are general-purpose AI tooling. The Customer is responsible for determining what data it submits. The Customer shall not submit special categories of Personal Data (Article 9 GDPR), data relating to criminal convictions and offences (Article 10 GDPR), or other particularly sensitive data into prompts, attachments or agent inputs unless this is strictly necessary, lawful, and consistent with appropriate safeguards. The Customer is encouraged to remove unnecessary identifiers from prompts and to send only the data required for the

relevant task.

5.4 Approval modes. Where the Services offer manual and auto-allow approval modes for actions taken by AI agents or the manager chat, the Customer is responsible for selecting the mode and permissions appropriate to its risk profile, and remains responsible for the supervision, validation and reversal of automated actions.

5.5 The Customer shall, where it acts as a processor on behalf of a third-party controller, ensure that it is authorised by that controller to appoint Corgent as a sub-processor on the terms of this DPA.

6. Subprocessors

6.1 The Customer provides **general written authorisation** for Corgent to engage Subprocessors to Process Customer Personal Data, subject to this Section 6. The Subprocessors engaged by Corgent as at the Effective Date are listed in **Annex III** , together with their role, location, transfer profile and erasure path. An up-to-date list is published at corgent.ai/subprocessors (the **“Subprocessor List”**).

6.2 Corgent shall impose, by way of a written contract, data protection obligations on each Subprocessor that are no less protective than those set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in accordance with Article 28(4) GDPR. Corgent remains fully liable to the Customer for the performance of each Subprocessor’s obligations.

6.3 Notice of changes. Corgent shall give the Customer at least **thirty (30) days’** prior notice of the addition or replacement of any Subprocessor, by updating the Subprocessor List and/or by notifying the Customer through the Services or by email, thereby giving the Customer the opportunity to object on reasonable data-protection grounds before the new Subprocessor begins Processing Customer Personal Data.

6.4 Objection. If the Customer objects in writing on reasonable data-protection grounds within fifteen (15) days of the notice, the Parties shall work together in good faith to find a mutually acceptable resolution. If no resolution is reached, the Customer may, as its sole and exclusive remedy, terminate the affected part of the Services in accordance with the Principal Agreement.

6.5 Customer-activated integrations (for example, Google or Microsoft) are engaged only where the Customer connects them and direct part of the data flow to the relevant provider acting on the Customer’s instructions; the Customer’s relationship with such providers may additionally be governed by the Customer’s own agreements with them.

7. Assistance with Data Subject Rights

7.1 Corgent shall promptly notify the Customer if it (or any Subprocessor) receives a request from a Data Subject to exercise rights of access, rectification, erasure, restriction, data portability, objection, or the right not to be subject to automated decision-making (a **“Data Subject Request”**) in respect of Customer Personal Data, and shall not respond to such request itself except on the documented instructions of the Customer or as required by law.

7.2 Taking into account the nature of the Processing, Corgent shall provide reasonable assistance, including by appropriate technical and organisational measures and through self-service functionality where available, to enable the Customer to respond to Data Subject Requests within the time limits set by Applicable Data Protection Laws.

7.3 Corgent operates a data subject access request (DSAR) workflow that coordinates primary deletion within Corgent-controlled systems and, where applicable, follow-up requests to relevant Subprocessors. Some Subprocessors require separate erasure requests after primary

deletion, as indicated in Annex III.

8. Personal Data Breach Notification

8.1 Corgent shall notify the Customer without undue delay, and in any event where feasible within **seventy-two (72) hours** , after becoming aware of a Personal Data Breach affecting Customer Personal Data, so as to enable the Customer to meet its own notification obligations under Articles 33 and 34 GDPR.

8.2 The notification shall, to the extent known and as information becomes available, describe the nature of the Personal Data Breach (including, where possible, the categories and approximate number of Data Subjects and records concerned); the likely consequences; the measures taken or proposed to address the breach and mitigate its effects; and the name and contact details of a relevant point of contact. Where it is not possible to provide all information at once, Corgent may provide it in phases without further undue delay.

8.3 Corgent shall take reasonable steps to contain, investigate and mitigate any Personal Data Breach, and shall reasonably cooperate with and assist the Customer in the Customer's investigation, notification and remediation. Corgent's notification of, or response to, a Personal Data Breach shall not be construed as an acknowledgement by Corgent of any fault or liability.

9. Security of Processing (Article 32 GDPR)

9.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk to the rights and freedoms of natural persons, Corgent shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in **Annex II** .

9.2 Corgent may update or modify the measures in Annex II from time to time, provided that such updates do not materially reduce the overall level of security of the Services during the term of the Principal Agreement.

9.3 Corgent shall ensure that access to Customer Personal Data is limited to personnel who require such access to perform the Principal Agreement, applying role-based access controls, least-privilege principles, and tenant isolation (including database row-level security) as further described in Annex II.

10. International Data Transfers

10.1 Corgent primarily hosts Customer Personal Data within the European Union (Supabase, Frankfurt region, eu-central-1). Corgent shall not transfer Customer Personal Data to a country outside the European Economic Area (**"EEA"**), the United Kingdom or Switzerland unless an appropriate transfer mechanism under Applicable Data Protection Laws is in place.

10.2 Where a transfer of Customer Personal Data from the EEA to a third country that is not the subject of an adequacy decision takes place (for example, to a U.S.-based monitoring Subprocessor, or to a model provider behind OpenRouter located outside the EU), the **Standard Contractual Clauses** apply and are incorporated into this DPA by reference, completed as set out in **Annex IV** . For transfers subject to UK Data Protection Laws, the **UK Addendum** applies; for transfers subject to the Swiss FADP, the SCCs apply with the modifications set out in Annex IV. Model inference via OpenRouter runs with Zero Data Retention (ZDR) and data_collection=deny; depending on the selected model, inference may take place on provider infrastructure outside the EU, covered by the Standard Contractual Clauses referenced in this clause.

10.3 By entering into this DPA, the Parties are deemed to have signed the Standard Contractual

Clauses (and, where applicable, the UK Addendum) as set out in Annex IV, as of the Effective Date. Where there is any conflict between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses prevail.

10.4 Corgent shall implement supplementary measures where necessary (such as encryption in transit and at rest, data minimisation, and contractual commitments restricting government access requests), and shall make available, on request, information reasonably necessary to demonstrate that transfers are conducted in accordance with Applicable Data Protection Laws. For model inference via OpenRouter, Corgent applies zero-data-retention (ZDR) and data_collection=deny as the standard configuration; third-country transfers arising from inference are covered by the Standard Contractual Clauses.

11. Audits, Information and Compliance

11.1 Corgent shall make available to the Customer all information reasonably necessary to demonstrate compliance with Article 28 GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.

11.2 In order to minimise disruption and protect the confidentiality and security of other customers, the Customer's audit rights are satisfied, in the first instance, by Corgent making available relevant documentation, security summaries, and any third-party certifications or audit reports (such as those held by its hosting and infrastructure Subprocessors). The Customer may request such materials no more than once per calendar year, except where required by a Supervisory Authority or following a Personal Data Breach.

11.3 Where the documentation provided under clause 11.2 is not sufficient to demonstrate compliance, the Customer may, on reasonable prior written notice of at least thirty (30) days, conduct an on-site or remote audit during normal business hours, subject to reasonable confidentiality and security requirements, and no more than once per calendar year. Each Party bears its own costs, save that the Customer shall reimburse Corgent's reasonable costs for assistance exceeding a de minimis level. The results of any audit are the Confidential Information of both Parties.

11.4 Corgent shall notify the Customer without undue delay if it determines that it can no longer meet its obligations under this DPA, in which case the Customer may suspend the transfer of Customer Personal Data and/or terminate the affected Services.

12. Return and Deletion of Customer Personal Data

12.1 Upon termination or expiry of the Principal Agreement, or at any time on the Customer's written request, Corgent shall, at the choice of the Customer, delete or return all Customer Personal Data and delete existing copies, unless Union or Member State law requires continued storage.

12.2 Corgent shall complete such deletion within a reasonable period not exceeding the retention windows described in Annex III, taking into account backup cycles. Customer Personal Data held in ephemeral caches and job queues is subject to time-to-live (TTL) expiry, typically within twenty-four (24) hours. Data retained for the establishment, exercise or defence of legal claims, or to comply with statutory retention obligations (for example, financial and tax records), shall be retained only for as long, and only to the extent, required, and shall remain subject to the protections of this DPA.

12.3 On request, Corgent shall certify in writing (which includes text form) that it has complied with this Section 12.

13. Liability and Indemnification

13.1 Each Party's liability arising out of or related to this DPA, whether in contract, tort or otherwise, is subject to the limitations and exclusions of liability set out in the Principal Agreement. Any reference in the Principal Agreement to the liability of a Party means the aggregate liability of that Party under the Principal Agreement and this DPA together.

13.2 Nothing in this DPA limits or excludes any liability that cannot be limited or excluded under Applicable Data Protection Laws, including the liability of the Parties to Data Subjects under Article 82 GDPR or the liability provisions of the Standard Contractual Clauses. As between the Parties, liability is allocated according to each Party's respective responsibility for the harm caused by the Processing.

14. Term, Variation and Survival

14.1 This DPA takes effect on the Effective Date and remains in force for as long as Corgent Processes Customer Personal Data on behalf of the Customer. Provisions that by their nature should survive termination (including those relating to confidentiality, deletion, transfers, liability and governing law) survive termination of this DPA and the Principal Agreement.

14.2 The Parties shall negotiate in good faith any amendments to this DPA that are required to address changes in Applicable Data Protection Laws, guidance from Supervisory Authorities, or the invalidation or replacement of any transfer mechanism. Corgent may update this DPA on reasonable notice where required to maintain compliance, provided that no such update materially diminishes the Customer's rights.

15. General Provisions

15.1 Governing law and jurisdiction. This DPA is governed by the laws of the Federal Republic of Germany, excluding the UN Convention on Contracts for the International Sale of Goods and its conflict-of-laws rules, without prejudice to any mandatory consumer protection law and to the governing-law and forum provisions of the Standard Contractual Clauses. The courts of the registered seat of Corgent have exclusive jurisdiction, to the extent permitted by law.

15.2 Notices. Data-protection notices to Corgent shall be sent to mk@corgent.ai. Notices to the Customer shall be sent to the contact details associated with the Customer's account or as otherwise set out in the Principal Agreement.

15.3 Severability. If any provision of this DPA is or becomes invalid or unenforceable, the remaining provisions remain in full force and effect, and the Parties shall replace the invalid provision with a valid provision that most closely reflects its commercial and legal intent.

15.4 Entire agreement. This DPA, together with its Annexes and the Standard Contractual Clauses, constitutes the entire agreement between the Parties with respect to the Processing of Customer Personal Data and supersedes any prior data-processing terms on the same subject matter.

15.5 Electronic execution. The Parties agree that acceptance of the Principal Agreement, or use of the Services after the Effective Date, has the same effect as signing this DPA and the Standard Contractual Clauses incorporated into it.

16. Corgent as Independent Controller (Account & Operational Data)

16.1 The Parties acknowledge that, in respect of certain limited data, Corgent acts as an independent controller and not as a processor. This includes account registration and

administration data, billing and credit data, authentication identifiers, security, abuse-prevention and audit logs, and aggregated or de-identified usage statistics used to operate, secure, and improve the Services (**“Account & Operational Data”**).

16.2 Corgent Processes Account & Operational Data in accordance with Applicable Data Protection Laws and its Privacy Policy, on legal bases including the performance of the contract (Article 6(1)(b) GDPR) and its legitimate interests in the secure, reliable and lawful operation of the Services (Article 6(1)(f) GDPR). Where required, Corgent obtains consent (Article 6(1)(a) GDPR), for example for non-essential analytics.

16.3 De-identified data. Where Corgent creates aggregated or de-identified data, it shall maintain and use such data only in de-identified form and shall not attempt to re-identify it, except as permitted by Applicable Data Protection Laws.

Agreed by the Parties

By accepting the Principal Agreement or by continuing to use the Services, each Party agrees to be bound by this DPA as of the Effective Date. Where a manual signature is required, the Parties may execute the DPA below.

For Corgent (Processor)	**For the Customer (Controller)**
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Entity: Malango Tech UG (haftungsbeschränkt) i.G.	Entity: _____
Date: _____	Date: _____

Annex I

Description of the Processing (SCC Annex I)

A. List of Parties

Data exporter / Controller: The Customer, as identified in the Principal Agreement and its account record. Role: controller (or processor acting for a third-party controller).

Data importer / Processor: Malango Tech UG (haftungsbeschränkt) i.G., trading as “Corgent”, Schumannstraße 24, 71640 Ludwigsburg, Germany. Contact: Maximilian Koch, mk@corgent.ai. Role: processor.

Activities relevant to the transfer: Provision of the Corgent AI agent platform and related Services to the data exporter.

B. Description of the Transfer

Categories of Data Subjects: The Customer’s authorised users; the Customer’s own end customers and contacts whose data the Customer submits; senders and recipients of content processed by agents (for example email or support contacts); and any other individuals whose Personal Data is contained in inputs the Customer chooses to submit.

Categories of Personal Data: Account and contact identifiers (name, email, role); authentication identifiers; prompts, attachments and agent inputs submitted by the Customer and any Personal Data contained therein; outputs generated by agents; integration content (for example, where connected, email or calendar data); usage, billing and transaction metadata; and technical/log data such as IP address and request metadata.

Special categories of data: Not intended. The Services are not designed for special categories of Personal Data (Article 9 GDPR) or criminal-offence data (Article 10 GDPR). Such data must not be submitted unless strictly necessary, lawful and subject to appropriate safeguards determined by the Customer (see clause 5.3).

Frequency of the transfer: Continuous, for the duration of the provision of the Services.

Nature of the Processing: Hosting, storage, transmission, routing to model providers for inference, execution of agent logic and integrations, caching and queuing, analytics (where enabled), error monitoring, billing computation, and deletion.

Purpose of the Processing: To provide, maintain, secure and support the Services in accordance with the Customer’s instructions and the Principal Agreement.

Duration of the Processing: For the term of the Principal Agreement and until deletion or return in accordance with Section 12, subject to statutory retention obligations.

Subprocessors: As set out in Annex III. The period for which sub-processors will process data corresponds to the duration above.

C. Competent Supervisory Authority

The competent Supervisory Authority is the lead authority for the data exporter (where the data exporter is established in the EEA), or otherwise the Supervisory Authority of the EEA Member State in which the data exporter’s EU representative is established. Where Corgent acts as exporter, the competent authority is the data protection authority of the German federal state of Baden-Württemberg (Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg).

Annex II

Technical and Organisational Measures (SCC Annex II · Art. 32 GDPR)

Corgent maintains the following technical and organisational measures to ensure a level of security appropriate to the risk. These measures may evolve, provided the overall level of protection is not materially reduced.

1. Pseudonymisation and encryption

- Encryption of Personal Data in transit using TLS (HTTPS/WSS) for all external connections.
- Encryption of Personal Data at rest for the primary database, object storage and backups provided by the hosting Subprocessor.
- Secrets, API keys and OAuth tokens are stored using encryption and access-controlled secret management; integration tokens are encrypted and revocable.
- Minimisation and, where feasible, pseudonymisation of identifiers in analytics and logs; sensitive payloads are excluded from analytics in production.

2. Confidentiality (access control)

- Role-based access control and least-privilege principles for personnel and services.
- Tenant isolation enforced at the application and database layer, including PostgreSQL row-level security (RLS).
- Authentication via a managed identity provider with JWT-based sessions; administrative access is restricted to a defined set of authorised user identifiers.
- Personnel are bound by confidentiality obligations and receive appropriate security and data-protection guidance.

3. Integrity

- Audit logging of security-relevant and administrative events, including consent changes and data subject request workflows.
- Input validation and schema validation (including for agent manifests and API requests) to reduce injection and abuse risks.
- Content security policy, transport-layer protections, and rate limiting to mitigate abuse and protect availability.

4. Availability and resilience

- Use of managed, redundant cloud infrastructure with automated backups for the primary datastore.
- Background workers and job queues with controlled retries; ephemeral cache and queue data is TTL-bound (typically ≤ 24 hours).
- Monitoring and error tracking to detect, analyse and resolve operational issues.

5. Restoration and testing

- Ability to restore availability and access to Personal Data from backups in a timely manner following an incident.
- Regular review of security configuration and dependency hygiene as part of the development lifecycle.

6. Governance, sub-processing and incident response

- A documented process for engaging and assessing Subprocessors, with contractual flow-down

of data-protection obligations.

- A Personal Data Breach response process designed to notify the Customer without undue delay (clause 8.1).
- A data subject request (DSAR) process coordinating primary deletion and Subprocessor follow-up.
- No undocumented “back doors” are built into the Services to provide third-party access to Personal Data.

Annex III

List of Subprocessors

The following Subprocessors are authorised to Process Customer Personal Data as at the Effective Date. The current list, including any updates, is published at corgent.ai/subprocessors. Integration Subprocessors marked “customer-activated” process data only where the Customer connects the relevant integration.

Subprocessor	Purpose & data categories	Region & transfer profile	Retention / erasure
Supabase	Core database, authentication and object-storage hosting. Account data, application records, auth identifiers, uploaded files.	European Union (Frankfurt, eu-central-1). Primary database and storage hosted in the EU.	Primary deletion path via Corgent account deletion and the DSAR workflow.
OpenRouter	Model routing and inference execution. Prompts, attachment metadata, model usage metadata.	OpenRouter (USA) with model providers in the EU and in third countries; inference location depends on the selected model. Zero-data-retention (ZDR) and data_collection=deny as standard; DPA with Standard Contractual Clauses in place.	Provider support workflow and contractual DPA channel.
Stripe	Credit purchase and payout processing. Billing identifiers, payment-method metadata, transaction metadata.	EU entity (Stripe Payments Europe, Ltd.) with standard contractual controls for onward transfers.	Processor-side retention bound to statutory finance obligations.
Resend	Transactional email delivery. Recipient email, message metadata, delivery logs.	EU region for the configured sending domain (eu-west-1) with provider safeguards.	Provider support request and retention-policy controls.
PostHog	Product analytics (only when analytics consent is granted). Pseudonymous identifiers, page views, feature-usage metadata.	EU Cloud (eu.i.posthog.com). EU-hosted; LLM payloads excluded in production.	Person deletion via PostHog API and consent withdrawal.
Sentry	Application error monitoring (only when performance consent is granted). Error telemetry; stack traces with PII stripped.	United States. Third-country processor under SCCs; PII stripped before transmission.	Issue-level deletion request and retention controls.
Railway	API and background-worker hosting. Request metadata, ephemeral queue payloads.	Europe (production region). Infrastructure processor; transient processing of API traffic.	Log-retention limits and infrastructure contract channel.
Netlify	Static frontend delivery and edge functions. HTTP access logs, CDN request metadata.	Global CDN edge. Edge-delivery processor under SCCs; no primary datastore.	Log retention per Netlify policy.
Redis (via Railway)	Ephemeral cache, job queues and rate-limit state. Session cache keys, TTL-bound queue job payloads.	Co-located with the Railway application region. Transient processing; TTL ≤ 24h.	Automatic TTL expiry and key deletion on account erasure.
Google (Gmail / Cloud) — *customer-activated*	Gmail and Google Cloud integrations when connected by the Customer. Email content, OAuth tokens, integration metadata.	Global (the Customer’s Google account region). Activated only when the Customer connects the integration.	Token revocation, Google account controls and Corgent deletion.

Microsoft Graph — *customer-activated*	Microsoft 365 integrations when connected by the Customer. Email/calendar metadata, OAuth tokens.	Global (the Customer's Microsoft tenant region). Activated only when the Customer connects the integration.	Token revocation, Microsoft account controls and Corgent deletion.

Subprocessor data-protection terms

- Supabase — supabase.com/legal/dpa
- OpenRouter — openrouter.ai/privacy
- Stripe — stripe.com/legal/dpa
- Resend — resend.com/legal/dpa
- PostHog — posthog.com/dpa
- Sentry — sentry.io/legal/dpa/
- Railway — railway.com/legal/dpa
- Netlify — netlify.com/legal/dpa/
- Google — cloud.google.com/terms/data-processing-addendum
- Microsoft — microsoft.com/licensing (Products and Services Data Protection Addendum)

Annex IV

Standard Contractual Clauses — Selections and Cross-Border Terms

1. EU Standard Contractual Clauses

Where the SCCs apply under Section 10, the SCCs (Implementing Decision (EU) 2021/914) are incorporated into this DPA and completed as follows:

- **Modules.** Module Two (Controller to Processor) applies where the Customer is a controller. Module Three (Processor to Processor) applies where the Customer is a processor acting for a third-party controller.
- **Clause 7 (Docking clause).** Applies.
- **Clause 9 (Use of sub-processors).** Option 2 (general written authorisation) applies. The minimum notice period for changes to sub-processors is thirty (30) days, as set out in clause 6.3 of this DPA.
- **Clause 11 (Redress).** The optional independent dispute-resolution mechanism does not apply.
- **Clause 17 (Governing law).** The SCCs are governed by the law of the Federal Republic of Germany.
- **Clause 18 (Choice of forum and jurisdiction).** Disputes are resolved before the courts of Germany.
- **Annex I, II and III to the SCCs.** Completed by Annex I, Annex II and Annex III of this DPA, respectively.

2. UK Addendum

For transfers subject to UK Data Protection Laws, the UK Addendum (version B1.0) is incorporated and applies to the SCCs. Table 1 (Parties) is completed by Annex I.A; Tables 2 and 3 are completed by reference to the EU SCCs and Annexes above; and in Table 4, neither Party may end the Addendum as set out in section 19, save where permitted by the Addendum. The “start date” is the Effective Date.

3. Swiss FADP

For transfers subject to the Swiss FADP, the SCCs apply with the following modifications: (i) references to the GDPR are to be understood as references to the Swiss FADP insofar as the transfer is governed by it; (ii) the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner (FDPIC); (iii) the term “Member State” must not be interpreted to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence; and (iv) the SCCs also protect the data of legal entities until the entry into force of equivalent revisions, to the extent required by the Swiss FADP.

4. Transfers from other jurisdictions

Where Personal Data is transferred subject to the data protection laws of another jurisdiction that requires an equivalent transfer mechanism, the SCCs apply with such modifications as are necessary to give effect to the equivalent protections required by that jurisdiction’s laws, and the relevant data exporter and importer roles are construed accordingly.

End of Data Processing Agreement. This document is generated programmatically by Corgent for transparency and contracting convenience. It is a template and does not constitute legal advice; the Customer should obtain its own advice on its specific circumstances.