Data Processing Agreement

(Auftragsverarbeitungsvertrag / AVV)

pursuant to Article 28 GDPR

Winkler Technologies GmbH

Achter de Knick 4, 24980 Schafflund, Germany

Represented by: Fabian Winkler, Geschäftsführer | fabian@myherald.io

Version 1.1 | Effective: May 2026

1. Parties and Scope

This Data Processing Agreement ("DPA") forms part of and is incorporated into the myHERALD Terms of Service ("Main Agreement") concluded between Winkler Technologies GmbH, Achter de Knick 4, 24980 Schafflund, Germany ("Processor" or "myHERALD") and the customer identified in the Main Agreement ("Controller" or "Customer").

This DPA reflects the parties' agreement on the processing of personal data by myHERALD on behalf of the Customer in connection with the myHERALD software-as-a-service platform ("Services"), in accordance with Article 28 of Regulation (EU) 2016/679 ("GDPR").

By accepting the Main Agreement, the Customer also accepts this DPA. In case of any conflict between this DPA and the Main Agreement, this DPA prevails with respect to data protection matters.

2. Definitions

Terms such as "personal data", "processing", "controller", "processor", "sub-processor", "data subject", and "supervisory authority" have the meaning given to them in Article 4 GDPR. "Standard Contractual Clauses" or "SCCs" means the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

3. Subject Matter, Nature, Purpose and Duration of Processing

Subject matter	Provision of the myHERALD social media operations platform, including AI-assisted content planning, research, drafting, review, image generation, and publishing to connected social channels.
Nature of processing	Storage, structuring, retrieval, transmission, generation, and erasure of personal data contained in Customer Data uploaded to or generated within the myHERALD platform.
Purpose of processing	Performance of the Services as agreed in the Main Agreement and as instructed by the Customer through use of the platform.
Duration	For the term of the Main Agreement and until all Customer Data has been deleted in accordance with Section 11.
Categories of data subjects	Customer's employees, users, contacts, prospects, third parties mentioned in uploaded knowledge base content, and audiences of published content.
Categories of personal data	Identifiers (name, email, user ID), professional data (job title, employer), account credentials (LinkedIn OAuth tokens), content uploaded by Customer (text, images, documents), AI-generated content, usage metadata, and any other personal data the Customer chooses to process via the Services.
Special categories	The Services are not intended for special categories of personal data within the meaning of Article 9 GDPR. The Customer shall not upload such data without prior written agreement.

4. Obligations of the Processor

myHERALD shall:

- process personal data only on documented instructions from the Customer, including with regard to transfers of personal data to a third country, unless required to do so by Union or Member State law to which myHERALD is subject;
- inform the Customer immediately if, in its opinion, an instruction infringes the GDPR or other applicable data protection provisions;

- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- implement the technical and organisational measures set out in Annex 2 (TOM) to ensure a level of security appropriate to the risk pursuant to Article 32 GDPR;
- respect the conditions for engaging sub-processors 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 for exercising data subject rights under Chapter III GDPR;
- assist the Customer in ensuring compliance with Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to myHERALD;
- at the choice of the Customer, delete or return all personal data after the end of the provision of services, and delete existing copies unless Union or Member State law requires storage of the personal data;
- make available to the Customer all information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, subject to Section 9.

5. Obligations of the Controller

The Customer warrants that:

- it has a valid legal basis for the processing of personal data via the Services and, where required, has obtained all necessary consents from data subjects;
- the instructions it provides to myHERALD comply with applicable data protection law;
- it shall not upload personal data that is excessive, unlawfully collected, or falls into special categories under Article 9 GDPR without prior written agreement;
- it is responsible for the accuracy, quality, and legality of Customer Data and the means by which it acquired such data.

6. Sub-processors

The Customer hereby grants myHERALD general written authorisation to engage sub-processors for the provision of the Services, subject to the following conditions:

- myHERALD maintains an up-to-date list of sub-processors in Annex 3 to this DPA, which is also published at https://myherald.io/sub-processors.
- myHERALD imposes data protection obligations on each sub-processor that are no less protective than those set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures.
- myHERALD shall inform the Customer of any intended changes concerning the addition or replacement of sub-processors with at least thirty (30) days' notice via email or in-product notification, thereby giving the Customer the opportunity to object to such changes on reasonable data protection grounds.
- If the Customer reasonably objects, the parties shall work in good faith to resolve the objection. If no resolution is reached, the Customer may terminate the affected Services with pro-rata refund of pre-paid fees.
- myHERALD remains fully liable to the Customer for the performance of the sub-processor's obligations.

7. International Data Transfers

Where myHERALD or any of its sub-processors processes personal data outside the European Economic Area, myHERALD ensures that such transfers are protected by an appropriate transfer mechanism under Chapter V GDPR, in particular:

- an adequacy decision of the European Commission (e.g. EU-U.S. Data Privacy Framework where applicable);
- the Standard Contractual Clauses (Module Two: Controller-to-Processor, or Module Three: Processor-to-Processor as applicable), incorporated by reference herein and considered executed between the parties for any transfer not covered by an adequacy decision;
- supplementary technical and contractual measures where required by a transfer impact assessment.

The list of sub-processors in Annex 3 indicates the country of processing and the applicable transfer mechanism.

Note on third-party integrations: Where the Customer connects its own accounts on third-party platforms (such as LinkedIn, X, Instagram, Facebook, TikTok, Reddit, Slack, or comparable services) to the myHERALD platform via OAuth or similar authentication, those third parties act as independent controllers in respect of the data the Customer chooses to publish to or retrieve from them. They are not sub-processors of myHERALD. myHERALD's role is limited to transmitting the Customer's instructions and content via the third party's API. The applicable terms and privacy policies of those third parties apply directly between the Customer and the third party.

8. Data Subject Requests and Personal Data Breaches

If myHERALD receives a request from a data subject in relation to Customer Data, myHERALD will, without undue delay, forward such request to the Customer and shall not respond to the data subject directly except on the Customer's documented instructions or as required by law.

myHERALD shall notify the Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a personal data breach affecting Customer Data. The notification shall contain the information set out in Article 33(3) GDPR insofar as such information is available to myHERALD, and shall be supplemented as further information becomes available.

9. Audits

myHERALD shall make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA and Article 28 GDPR. To satisfy audit rights under Article 28(3)(h) GDPR, myHERALD shall, upon written request and no more than once per calendar year (except in the event of a personal data breach or supervisory authority order), provide:

- its current TOM document (Annex 2);
- a written response to a reasonable security questionnaire submitted by the Customer;
- any third-party audit reports or certifications it holds (e.g. SOC 2, ISO 27001) where available.

On-site audits shall be conducted only if the above documentation is insufficient and shall be carried out during business hours, with at least thirty (30) days' prior written notice, by an independent auditor bound by confidentiality, in a manner that does not unreasonably disrupt myHERALD's operations. The Customer shall bear its own audit costs.

10. Liability

The liability of the parties under this DPA is governed by the limitations of liability set out in the Main Agreement, except where applicable law prohibits such limitation. Article 82 GDPR remains unaffected.

11. Term, Termination, Deletion and Return

This DPA enters into force upon acceptance of the Main Agreement and remains in effect for as long as myHERALD processes personal data on behalf of the Customer.

Upon termination of the Main Agreement, the Customer may export its data through the in-product export functionality for a period of thirty (30) days. Thereafter, myHERALD shall delete all Customer Data, including backups, within a further sixty (60) days, unless retention is required by Union or Member State law. myHERALD shall confirm deletion in writing upon written request.

12. Final Provisions

Should any provision of this DPA be held invalid or unenforceable, this shall not affect the validity of the remaining provisions. The parties shall replace the invalid or unenforceable provision with one that comes closest to the intended economic and legal purpose.

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. Exclusive place of jurisdiction is Flensburg, Germany, to the extent legally permissible.

Annex 1 — Description of Processing

This Annex specifies the details of the processing as required by Article 28(3) GDPR. The information in Section 3 of this DPA forms part of this Annex.

Processing operations

- Authentication and account management of Customer users on the myHERALD platform.
- Storage of Customer-uploaded knowledge base documents and generation of vector embeddings.
- AI-assisted research, drafting, review and image generation for social media content.
- Publishing of approved content to social media platforms via OAuth-connected accounts.
- Logging of agent runs and usage metrics for billing, debugging and security.

Frequency

Continuous, for the duration of the Main Agreement.

Annex 2 — Technical and Organisational Measures (TOM)

myHERALD implements the following technical and organisational measures pursuant to Article 32 GDPR. The measures may evolve over time; myHERALD reserves the right to update them, provided the level of protection is not reduced.

1. Confidentiality

- Access control: Supabase Auth with bcrypt-hashed passwords; Google OAuth as alternative login. Workspace-scoped Row Level Security (RLS) on all tables. Role-based access control (admin, member).
- Authorisation: principle of least privilege; no shared accounts; service-role keys stored only in server-side environment variables.
- Confidentiality obligations: all personnel and contractors are bound by written confidentiality obligations.
- Pseudonymisation and encryption: knowledge base content embedded as numerical vectors; OAuth tokens encrypted at rest.

2. Integrity

- Encryption in transit via TLS 1.2+ for all client-server and server-sub-processor communication.
- Encryption at rest via Supabase managed AES-256 encryption (eu-central-1 region).
- Audit logging of agent runs (token usage, costs, actions) in the agent_runs table.
- Input validation and parameterised database queries to prevent injection.

3. Availability and Resilience

- Daily automated backups via Supabase, retained according to Supabase's backup policy.
- Hosting in eu-central-1 (Frankfurt) for primary database and storage.
- Uptime monitoring and error tracking.

4. Procedures for regular testing, assessing and evaluating

- Dependency vulnerability scanning.
- Periodic review of access rights and sub-processor list.
- Incident response process aligned with Article 33 GDPR (72-hour notification).

5. Sub-processor management

- Vetting of all sub-processors for GDPR compliance prior to engagement.
- Written DPAs with all sub-processors, including SCCs for non-EEA transfers.
- Public sub-processor list with change notifications.

6. Data minimisation, retention and deletion

- Soft deletion with 30-day purge for content items and knowledge base entries.
- Account deletion within 30 days of request.
- Retention periods documented in the Records of Processing Activities.

Annex 3 — List of Sub-processors

The following sub-processors are engaged by myHERALD in the provision of the Services as of the effective date of this DPA. The current list is also maintained at https://myherald.io/sub-processors.

Sub-processor	Purpose	Location	Transfer mechanism
Supabase Inc.	Database, authentication, file storage, vector search	EU (Frankfurt)	EEA — no transfer
Anthropic PBC	AI model (Claude) for content generation and orchestration	USA	SCCs (Module 3) + DPA
Google LLC	AI model (Gemini) for image generation and URL fetching	USA	DPF + SCCs + DPA
Voyage AI (MongoDB, Inc.)	Embedding generation for knowledge base	USA	SCCs + DPA
Loops.so (Astrodon Corp.)	Marketing email delivery and unsubscribe management	USA	SCCs + DPA
Resend (Plus Five Five Inc.)	Transactional email delivery	USA	DPF + SCCs + DPA
Stripe Inc.	Payment processing for subscriptions	USA	DPF + SCCs + DPA
PostHog Inc.	Product analytics	EU (Frankfurt)	EEA — no transfer
Railway Corp.	Application hosting (Next.js dashboard)	EU West (Amsterdam)	EEA — no transfer

Last updated: May 2026