Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR · Heylog FlexCo · Version 2.5 (Final)

Document ID / version	DPA-001 · v2.5 (Final)
Processor	Heylog FlexCo, Wiedner Gürtel 13, Icon Tower 24/3, 1100 Vienna
Controller	see Annex I (to be completed by the Controller)
Data protection / DPO	gdpr@heylog.com
Legal basis	Art. 28 GDPR
Governing law	Austria
Entry into force	1 September 2026
Annexes	I Parties · II Processing · III Sub-processors · IV TOMs · V Storage/transfer

Based on the existing DPA (as of October 2025) and Art. 28 GDPR, harmonised for Heylog FlexCo. Approved version, effective from 1 September 2026.

Definitions

The terms used in this agreement (including personal data, processing, controller, processor, data subject, supervisory authority) have the meaning given in Art. 4 GDPR. “Sub-processor” means a further processor engaged by the Processor. “Customer data” means the personal data processed by the Processor on behalf of the Controller.

Section 1 Subject matter, nature and duration

This agreement specifies the obligations under Art. 28(3)–(4) GDPR for the processing of personal data carried out by the Processor (Heylog FlexCo) on behalf of the Controller. The subject matter, nature, scope, purpose and duration of the processing result from the underlying main contract and from Annex II. The agreement applies for the term of the main contract. The Controller is responsible for the lawfulness of the processing and the admissibility of its instructions; it holds the rights of instruction, review and audit set out in this agreement.

Section 2 Obligations of the Processor

- **Bound by instructions —** processing exclusively on documented instructions from the Controller; notification if an instruction infringes data protection law. Documented instructions are given in text form to the data protection contact (gdpr@heylog.com); verbal instructions are confirmed in text form without delay.
- **Purpose limitation —** processing only for the purposes set out in Annex II.
- **Confidentiality —** persons bound to confidentiality; access limited to what is necessary to provide the service.
- **Technical and organisational measures (Art. 32) —** implementation in accordance with Annex IV (TOMs).
- **Sub-processors —** engagement only with prior (general) written authorisation; the authorised sub-processors are listed in Annex III and kept up to date; the current version is additionally available for download at heylog.com/datenverarbeitung. The Controller is informed of intended changes (new or replaced sub-processors) at least 30 days in advance and may object within this period on important data protection grounds. Until a justified objection has been resolved, the sub-processor concerned is not used productively for the Controller's data; if no agreement or equivalent alternative is reached, the Controller has an extraordinary right of termination with regard to the affected services. Sub-processors are placed under equivalent data protection obligations; the Processor is liable for their compliance.
- **Third-country transfers —** only on documented instructions or lawfully in accordance with Chapter V GDPR (EU-US Data Privacy Framework, where certified, or EU Standard Contractual Clauses 2021/914 with supplementary safeguards).
- **Government access requests —** legally compelled requests from authorities for the Controller's data are forwarded to the Controller without delay, insofar as legally permissible; no data is disclosed without legal review, and manifestly unlawful orders are challenged. Sub-processors are placed under corresponding obligations.

- **Support for the Controller —** with data subject rights (requests are forwarded without delay; support provided in good time so that the Controller can meet its statutory deadlines), data protection impact assessments and the obligations under Art. 32–36 GDPR.
- **Notification of personal data breaches —** notification without culpable delay, at the latest within 48 hours of becoming aware (initial notification also where the facts are not yet complete), including a description, the categories/numbers affected, contact person, consequences and remedial measures. On request, the Processor supports the Controller in notifying the supervisory authority and the data subjects (Art. 33/34).
- **Evidence and audits —** provision of the information required as evidence; where available, suitable evidence (including certificates/reports of the providers used, ISMS documentation) may replace an on-site audit; reviews/audits no more than once a year and where there is specific cause, with reasonable advance notice; the costs of a review are borne by the Controller.
- **Deletion/return —** at the Controller's choice, deletion or return of the data (return in a commonly used machine-readable format) within 30 days of the end of the processing — including deletion at all sub-processors and in backups once the rotation cycle has elapsed — unless a statutory retention obligation prevents this; deletion is confirmed in writing.

Section 3 Final provisions

- **Liability —** in accordance with Art. 82 GDPR and the provisions of the main contract.
- **Precedence —** in the event of conflicts, this agreement takes precedence over the data protection provisions of the main contract.
- **Amendments and versioning —** amendments to this agreement require text form. The Processor gives reasonable notice of adjustments due to changed legal requirements or processing operations; the version in force is identified by version number and date in the document header.
- **Governing law and jurisdiction —** Austrian law applies; the place of jurisdiction is as set out in the main contract.

Annex I — Parties

Controller — to be completed by the Controller: name/company: _____ · address: _____ · represented by: _____ · data protection contact: _____.

Processor: Heylog FlexCo, Wiedner Gürtel 13, Icon Tower 24/3, 1100 Vienna, Austria. Data protection contact: gdpr@heylog.com.

Annex II — Description of the processing

Data subjects

Employees of the Controller; contracted transport companies and their employees (drivers/dispatchers); customers of the Controller.

Categories of personal data

Employees/carriers: name, contact details, usage data (logs, metadata), communication content (messages, transcripts where applicable). Customers: name, date of birth where applicable, address, service-related data. Location/GPS data: only in customer-specific configured workflows and only after approval by the Controller (not a default, no blanket tracking). Special categories (Art. 9 GDPR): not processed intentionally; incidental occurrence in free text/transcripts cannot be ruled out and is treated with the same protective measures.

Nature, scope and purpose

Digital processing via the Heylog system to enable and simplify communication between drivers and dispatchers (order assignment, management and status tracking of transports). Location-based features are provided only in customer-specific configured workflows and after approval by the Controller.

AI-assisted features (e.g. transcription of meetings, translation) may form part of the service and, where offered, are provided by default; they can be disabled or restricted at the Controller's request. Disabling them may affect the scope of services and the fee; details are governed by the main contract. Where such features are used, processing takes place via the sub-processors listed in Annex III.

Heylog itself does not process the Controller's personal data for AI training purposes. The scope of processing by AI sub-processors is governed by their respective data processing agreements. Participants

are informed about the use of AI-assisted transcription in accordance with Art. 50 of the AI Act (Regulation (EU) 2024/1689); no emotion or sentiment analysis takes place.

Duration

For the term of the main contract and for as long as the processing is necessary, or until the Controller instructs that it be ended.

Annex III — Authorised sub-processors

Sub-processor	Purpose	Version	Location/Region	Transfer
Amazon Web Services (AWS)	Hosting / infrastructure	V2	EU	DPF/SCC
Supabase	Hosting / database	V3	EU	EU/SCC
Cloudflare	CDN / proxy / WAF	V2, V3	US/EU	DPF/SCC
WhatsApp Business API (Meta)	Chat with drivers/dispatchers	V2, V3	EU/US	DPF/SCC
Twilio	Messaging (SMS/voice/API)	V2, V3	EU/US	DPF/SCC
DeepL	Translation of messages	V2, V3	EU (DE)	EU
Google AI Translate	Translation (optional)	V2, V3	EU/US	DPF/SCC
Firebase (Google)	App geodata / push	V2, V3	EU/US	DPF/SCC
Google Maps Platform	Maps / geocoding / routing	V2, V3	EU/US	DPF/SCC
SRG IT & Marketing GmbH	Data integration / middleware	V2, V3	AT/EU	EU
Google Workspace	Collaboration (incl. support access)	V2, V3	EU/US	DPF/SCC
Pusher	Realtime API (websockets)	V2	EU/US	DPF/SCC
Brevo (Sendinblue)	System/user emails	V2	EU (FR)	EU
SMTP2GO	Transactional email delivery	V3	US/EU	DPF/SCC
Sentry	Application error tracking	V3	EU/US	DPF/SCC
Read.ai	Transcription (external meetings, opt-out)	V2, V3	US/EU	DPF/SCC
Anthropic (Claude)	AI processing of transcripts	V2, V3	US/EU	DPF/SCC

“Location/Region” refers to the provider's place of business or processing region; customer data is primarily held at rest in the EU (AWS/Supabase, EU region). For providers with a US nexus, transfers are based on the EU-US Data Privacy Framework (where the provider is certified) and/or the EU Standard Contractual Clauses (2021/914, module 2 or 3) with supplementary safeguards (encryption, EU-side key management, EU data residency where possible). The provider-specific transfer basis, the categories of data processed and the transfer impact assessments are maintained in the internal processor register and made available to the Controller on request. A DPA is in place with every sub-processor. GCP will be removed after the V2→AWS migration. Note: “V3” = Heylog Operations System, “V2” = legacy platform (being migrated).

Annex IV — Technical and organisational measures (Art. 32 GDPR)

Heylog does not operate its own data centre; production runs with certified cloud providers (AWS for V2, Supabase for V3; EU region). Physical infrastructure security is ensured by these providers (ISO 27001 / SOC 2). Heylog is preparing for Cyber Trust certification. Customer data is stored in the EU wherever this is technically possible (overview by provider: Annex V). Heylog's own measures:

Confidentiality

- Physical access control: private office at the factory300 campus (Peter-Behrens-Platz 10, 4020 Linz), entry only for Heylog employees with a keycard; keycards issued only after registration/notification; visitors must register and be accompanied.
- System access control: individual user accounts, password policy (at least 8 characters), MFA for critical/administrative access (in V3 additionally enabled for users by the workspace owner), automatic screen lock, full-disk encryption on laptops (implemented).
- Data access control: role-based least-privilege concept, separate admin/user accounts, logging, encryption of data at rest (AES).
- Separation control: tenant/workspace separation; separate development, staging and production environments.

Integrity

- Transfer control: TLS 1.3 in transit; encrypted transmission; no unencrypted transmission of sensitive data.
- Input control: logging of entry/modification/deletion with attribution to individuals; deletion requests to gdpr@heylog.com.

Availability and resilience

- Cloud hosting with AWS (V2) / Supabase (V3), EU region, with provider-side redundancy; backups + annual restore test; cyber insurance (proof of cover on request).
- Monitoring and alerting in operation (including application error tracking via Sentry).

Procedures for regular review

- Record of processing activities (RoPA) and ISMS reviewed at least annually; documented incident response process; processor control via DPAs with all sub-processors; designated data protection contact (gdpr@heylog.com).
- External penetration test of the Driver & Yard Operations System planned (second half of 2026).

Annex V — EU data residency & transfer basis

Sub-processor	EU data residency	Transfer basis
Amazon Web Services (AWS)	EU (configured)	DPF / SCC
Supabase	EU	EU / SCC
Cloudflare	EU (configured)	DPF / SCC
WhatsApp Business API (Meta)	partly US	DPF / SCC
Twilio	EU (configured)	DPF / SCC
DeepL	EU (Germany)	EU
Google AI Translate	EU (configured)	DPF / SCC
Firebase (Google)	partly US / limited	DPF / SCC
Google Maps Platform	global (processing)	DPF / SCC
SRG IT & Marketing GmbH	AT / EU	EU
Google Workspace	EU (configured)	DPF / SCC
Pusher	EU/US (cluster)	DPF / SCC
Brevo (Sendinblue)	EU (France)	EU
SMTP2GO	EU (configured)	DPF / SCC
Sentry	EU (configured)	DPF / SCC
Read.ai	partly US / limited	SCC
Anthropic (Claude)	partly US / limited	SCC

Principle: customer data is stored in the EU wherever this is technically possible. "EU (configured)" = EU region/data localisation active or activatable; "partly US / limited" = no full EU data residency available from the provider. Transfer basis: EU-US Data Privacy Framework where the provider is certified, otherwise EU Standard Contractual Clauses (2021/914). Provider-specific confirmation takes place in the course of DPA procurement.

Execution

This agreement takes effect upon signature by both parties; Annexes I–V form part of the agreement. It is concluded in two identical counterparts.

Controller	Processor
Place, date: _____	Place, date: _____
Name: _____	Name: _____
Position: _____	Position: _____
Signature:	Signature:
_____	_____