

Data Processing Agreement

Article 28 GDPR · Version 1.0 · 12 September 2026 · Governed by Dutch law · Controller fields are for completion on signature.

Agents In White · Private AI Intelligence Studio

Version 1.0 · 12 September 2026

This Data Processing Agreement ("DPA") forms part of the Engagement between the Client and AIW Systems Europe B.V., trading as Agents In White, and implements Article 28 of Regulation (EU) 2016/679 ("GDPR"). Where it conflicts with other parts of the Engagement on the subject of personal data, this DPA prevails.

Parties

Controller: the client named in the Engagement — legal name, registered address, and registration number as stated in the signature block below and in the statement of work

Processor: AIW Systems Europe B.V., trading as Agents In White, Alphen aan den Rijn, Netherlands, Chamber of Commerce (KvK) number supplied on request and stated on every contract and invoice

Processor contact for data protection: admin@agentsiw.com

1. Roles

1.1 The Controller determines the purposes and means of processing. AIW processes personal data only on the Controller's documented instructions.

1.2 The Engagement, its statement of work, Annex 1, and the Controller's written configuration decisions together constitute those instructions.

1.3 AIW informs the Controller without undue delay if an instruction, in AIW's opinion, infringes the GDPR or other data protection law, and may suspend the affected processing until the instruction is confirmed or amended.

1.4 Where AIW determines purposes of its own — for example its own client administration — it acts as controller and its own Privacy Policy applies.

2. Subject Matter, Duration, And Scope

2.1 Subject matter, nature, purpose, categories of data subject, and categories of personal data are specified in **Annex 1**.

2.2 Processing lasts as long as the Engagement, plus any return or deletion period under §10.

2.3 AIW processes no personal data beyond what the Engagement requires and does not process it for its own purposes, for profiling, for enrichment, or for any commercial purpose of its own.

3. Confidentiality

3.1 AIW ensures that every person authorised to process personal data is bound by a written confidentiality obligation that survives the end of their engagement with AIW.

3.2 Access is granted on a need-to-know, least-privilege basis and is reviewed at least quarterly and revoked on role change or departure.

4. Security

4.1 AIW implements appropriate technical and organisational measures under Article 32 GDPR, described in **Annex 2**.

4.2 AIW reviews these measures periodically and may change them, provided the level of protection is not reduced.

4.3 The Controller is responsible for the security of systems, credentials, and environments under its own control, and for configuration choices it makes or requires.

5. Sub-Processors

5.1 The Controller grants general authorisation for AIW to engage sub-processors. Those in use are listed at /legal/sub-processors and in **Annex 3**.

5.2 AIW gives the Controller at least 14 days' written notice — by email or by notified update to the published list — before adding or replacing a sub-processor.

5.3 The Controller may object on reasonable, documented data protection grounds within that period. The parties will seek a workable alternative in good faith. If none is available and the sub-processor is essential, either party may terminate the affected part of the Engagement without penalty, against payment for work performed.

5.4 AIW imposes on each sub-processor data protection obligations no less protective than this DPA and remains fully liable to the Controller for its sub-processors' performance.

5.5 **Model Providers** engaged in a Deliverable are sub-processors where they process personal data. AIW selects, where the provider offers it, configurations that exclude Controller data from provider model training and that apply zero or minimal retention.

6. AI-Specific Commitments

6.1 AIW does not use personal data processed under this DPA to train, fine-tune, or evaluate any model made available beyond the Controller's own environment.

6.2 Where a Deliverable produces personal data as Output, that Output is personal data under this DPA and subject to the same obligations.

6.3 AIW does not deploy automated decision-making with legal or similarly significant effect on data subjects unless the statement of work provides for it expressly, in which case the Controller is responsible for the Article 22 GDPR basis, the safeguards, and the information given to data subjects.

6.4 On request, AIW provides the technical information reasonably available to it to support the Controller's data protection impact assessment, its records under Article 30, and its transparency obligations under the EU AI Act.

6.5 Prompts, logs, traces, and evaluation sets that contain personal data are treated as personal data, retained no longer than needed for operation and debugging, and pseudonymised or redacted where operationally feasible.

7. International Transfers

7.1 AIW preferentially processes personal data within the European Economic Area.

7.2 Transfers to a third country take place only where covered by an adequacy decision under Article 45 GDPR, or by the Standard Contractual Clauses of Commission Implementing Decision (EU) 2021/914 with a transfer impact assessment and supplementary measures including encryption in transit and at rest.

7.3 Where the Controller requires the SCCs to be concluded directly, the parties will execute them; Module Two (controller to processor) applies, with the Netherlands as the governing law and the

Rechtbank Den Haag as the forum, and Annexes 1 to 3 of this DPA populating their annexes.

7.4 AIW notifies the Controller if it receives a legally binding request from a public authority for personal data processed under this DPA, unless prohibited from doing so, and challenges disproportionate requests where legal grounds exist.

8. Personal Data Breach

8.1 AIW notifies the Controller without undue delay, and in any event within 24 hours, of becoming aware of a personal data breach affecting personal data processed under this DPA.

8.2 The notification states, as far as known: the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, the measures taken or proposed, and a contact point. Information not yet available is supplied in phases without further undue delay.

8.3 AIW assists the Controller in meeting its Articles 33 and 34 obligations. AIW does not notify a supervisory authority or data subjects on the Controller's behalf unless instructed in writing.

8.4 AIW documents all breaches, including remedial action.

9. Data Subject Rights And Assistance

9.1 AIW does not respond directly to data subject requests concerning the Controller's data. Requests received are forwarded to the Controller without undue delay and in any event within 3 business days.

9.2 AIW assists the Controller in honouring rights of access, rectification, erasure, restriction, portability, and objection, using the technical means available in the relevant system.

9.3 AIW assists with data protection impact assessments and prior consultation under Articles 35 and 36 to the extent the processing is within AIW's sphere.

9.4 Assistance within reasonable limits is included. Assistance requiring substantial engineering effort, or repeated assistance caused by the Controller's own configuration, is chargeable at AIW's standard rates after written notice.

10. Return And Deletion

10.1 On termination of the Engagement, or earlier on written instruction, AIW returns the personal data in a commonly used machine-readable format, or deletes it, at the Controller's choice.

10.2 Deletion is completed within 30 days of the instruction, except for copies in routine backups, which are deleted in the ordinary rotation and within a maximum of 90 days, and remain subject to this DPA until deleted.

10.3 AIW may retain personal data where Union or member state law requires it, informing the Controller of the requirement.

10.4 AIW confirms completion of deletion in writing on request.

11. Audit And Records

11.1 AIW makes available the information necessary to demonstrate compliance with this DPA.

11.2 The Controller may audit once per 12-month period, on 30 days' written notice, during business hours, without disrupting operations, and subject to confidentiality. AIW may satisfy an audit request by providing an up-to-date third-party report, certification, or completed security questionnaire where these reasonably address the scope.

11.3 An additional audit may be conducted following a personal data breach affecting the Controller's data or a documented compliance concern.

11.4 The Controller bears its own audit costs and AIW's reasonable costs of supporting an on-site audit.

12. Liability

Liability under this DPA is subject to the limitations in the General Terms of Engagement, except that those limitations do not restrict any liability of AIW towards a data subject or a supervisory authority under Article 82 GDPR or under a statutory administrative fine imposed on AIW for its own conduct.

13. Term, Law, And Forum

13.1 This DPA takes effect with the Engagement and ends when processing and deletion are complete.

13.2 Dutch law governs this DPA. Disputes go exclusively to the Rechtbank Den Haag, Netherlands.

13.3 AIW may amend this DPA to reflect changes in law, guidance from a supervisory authority, or its own infrastructure, provided the level of protection is not reduced and the Controller is notified 30 days in advance.

Annex 1 — Processing Details

Subject matter	Design, development, deployment, and operation of private AI systems, agents, automations, and portals for the Controller
Nature of processing	Collection, structuring, storage, retrieval, consultation, use, transmission via API, generation of Output, pseudonymisation, erasure
Purpose	Delivery and operation of the Deliverable described in the statement of work
Duration	Term of the Engagement plus the deletion period in §10
Categories of data subject	The Controller's employees, contractors, clients and their contacts, leads and prospects, candidates, suppliers, and end users of the Deliverable. Narrowed or extended only in the statement of work.
Categories of personal data	Identification and contact data; employment and role data; correspondence content; document content; CRM and transaction records; usage and log data; prompts and Output containing any of the foregoing.
Special categories	None. Special categories are processed only where the statement of work names them expressly and records the additional safeguards agreed in writing.
Frequency	Continuous during operation; batch during development and migration
Retention within the system	As configured in the statement of work. Where no period is configured: operational records for the term of the Engagement, prompts and model logs for 30 days, system and access logs for 12 months, backups for 35 days.

Annex 2 — Technical And Organisational Measures

Access control — Named accounts only; no shared credentials. Multi-factor authentication on all administrative and repository access. Least-privilege roles. Quarterly access review. Immediate revocation on departure.

Encryption — TLS 1.2 or higher in transit. AES-256 or equivalent at rest. Secrets held in a managed secret store, never in source code or chat.

Segregation — Separate environments and credentials per client. No shared production databases across clients. Development and test environments use synthetic or pseudonymised data wherever feasible.

Logging and monitoring — Administrative and system access logged; logs protected against modification; anomaly alerting on authentication and data-export events.

Resilience — Encrypted backups with defined recovery objectives per Engagement; restore testing; documented incident response procedure with a named owner.

Change management — Version control, peer review of changes to production, and rollback capability.

Device and endpoint security — Full-disk encryption, automatic screen lock, maintained operating systems, endpoint protection on all devices used for delivery.

Personnel — Written confidentiality undertakings, need-to-know access, and data protection instruction for everyone involved in delivery.

AI-specific — Provider no-training and minimal-retention configuration where offered; prompt and log minimisation; redaction of identifiers where operationally feasible; guardrails and human-in-the-loop checkpoints on consequential Output.

Sub-processor governance — Written data protection terms with every sub-processor, maintained register, and change notification to the Controller.

Deletion — Documented, verifiable deletion procedure covering primary storage, derived artefacts, prompts, logs, and backups.

Annex 3 — Approved Sub-Processors

The list in force is published at </legal/sub-processors> and incorporated here by reference. Sub-processors specific to this Engagement:

Sub-processor	Role	Location	Transfer mechanism
Cloudflare	Application hosting and edge delivery	EEA	EEA processing; EU Standard Contractual Clauses where applicable
Hostinger Mail	Transactional and business email	EEA	EEA processing; EU Standard Contractual Clauses where applicable
Managed cloud database and object storage provider	Application database and file storage	EEA	EEA processing; EU Standard Contractual Clauses where applicable
OpenAI, Anthropic, Google	Foundation model inference and embeddings, where the Deliverable requires inference	EEA where offered, otherwise United States	Adequacy decision or EU Standard Contractual Clauses; no-training and minimal-retention settings applied where the provider offers them

Any sub-processor beyond this default set is added only under §5 of this Agreement, with prior written notice to the Controller.

Signatures**Controller** — complete on execution

Legal name: _____

Name: _____ · Title: _____ · Date:

Signature: _____

Processor — AIW Systems Europe B.V. (Agents In White)

Name: Ommar Abou Heweita · Title: Founder & Chief Executive Officer · Date:

Signature: _____