Data Processing Agreement

(DPA) in accordance with Art. 28 GDPR

Data Controller: **[CUSTOMER NAME / COMPANY]** Data Processor: **All Media FlexCo**

Note: This is the English version of this document. In the event of any discrepancies between the German and English versions, the German version shall prevail.

Table of Contents

§ 1 Subject Matter and Duration of Processing

1.1 This Data Processing Agreement (DPA) specifies the data protection rights and obligations of the parties in relation to the processing of personal data by the Data Processor on behalf of the Data Controller in accordance with Art. 28 GDPR.

1.2 The Data Processor processes personal data exclusively on the instructions and basis of documented instructions from the Data Controller.

1.3 The duration of processing is determined by the term of the underlying main contract (framework agreement, service agreement, SaaS agreement).

1.4 Duration of processing: For the duration of the respective contract or main agreement as agreed between the parties.

Art. 28 GDPR

§ 2 Nature and Purpose of Processing

2.1 Purpose of processing (tick as appropriate):

- Software development and maintenance
- AI-enabled data processing and analytics
- IT consulting and project management
- SaaS provision and hosting
- Support and maintenance of existing systems
- Other: _____

2.2 Categories of personal data (tick as appropriate):

- Communication data (email, telephone, correspondence, chat logs, attachments/files)
- Technical data (log files, IP addresses, browser data, device information)
- Contract and billing data (invoices, payment information, contracts)
- Master data (name, address, contact information)
- Employee data (employment contracts, payroll information, time tracking)
- Health data (information about illness, findings, medical certificates)
- Applicant data (application documents, CV data, references)
- Other: _____

2.3 Categories of data subjects (tick as appropriate):

- End customers of the Data Controller (buyers, clients, customers)
- Employees of end customers (staff, representatives, project staff)
- Contacts (project managers, decision-makers, account managers)
- Communication partners (external service providers, suppliers, partners)
- Employees of the Data Controller (internal staff, developers, project team)
- Job applicants (application documents, CV data)
- Suppliers (contractors, subcontractors, distributors)
- Other: _____

§ 3 Obligations of the Data Processor

The Data Processor undertakes in particular to:

3.1 Process personal data exclusively on the basis of documented instructions from the Data Controller, unless processing is required under Union law or the law of a Member State. In such a case, the Data Processor shall inform the Data Controller of this legal requirement before processing.

3.2 Ensure that all persons involved in processing are bound by confidentiality obligations or are subject to an appropriate statutory duty of confidentiality.

3.3 Implement appropriate technical and organisational measures in accordance with Art. 32 GDPR (see § 4).

3.4 Processing of personal data for its own purposes is excluded.

3.5 Notify the Data Controller without undue delay, but no later than within 48 hours of becoming aware of any breach of personal data protection (data breach) in accordance with Art. 33 GDPR. The notification shall contain at least: the nature of the breach, the affected categories of data and groups of data subjects, the likely consequences and the measures taken.

3.6 The Data Processor shall name its data protection officer (if any) and provide its contact details to the Data Controller in writing.

Art. 28, 32, 33 GDPR

§ 4 Technical and Organisational Measures (TOMs)

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of processing as well as the varying probability and severity of the risks to the rights and freedoms of natural persons, the Data Processor shall implement appropriate technical and organisational measures in accordance with Art. 32 GDPR.

4.2 The specific technical and organisational measures are documented in Annex 2 (Technical and Organisational Measures -- TOMs) to this DPA. Annex 2 is an integral part of this DPA.

4.3 The measures shall include in particular: access control, entrance control, access control, disclosure control, input control, instruction control, availability control, separation control as well as organisational and AI-specific measures.

4.4 Technical and organisational measures are subject to technical progress and further development. The Data Processor may implement alternative measures provided that the level of security is not compromised.

Art. 32 GDPR

§ 4a Use of AI Systems in Contract Processing

4a.1 It is in the nature of the services rendered that within the scope of contract processing, personal data may be transmitted to AI systems (e.g. OpenAI, Google Gemini, Anthropic

Claude, Mistral) and processed by these. This occurs exclusively via the providers' platform API access, where the transmitted data is generally not used for model training.

4a.2 If the Data Controller explicitly does not wish personal data to be transmitted to AI systems, this must be stated in writing as part of this Data Processing Agreement or in a separate order. In this case, the Data Processor is obliged to use alternative processing methods without AI connection, insofar as this is technically feasible and economically reasonable.

4a.3 The current status of opt-out from model training at the AI providers used can be found in the Sub-Processor List (Annex 1 or Sub-DPA).

4a.4 Where desired and appropriate, personal data shall be anonymised or pseudonymised before transmission to AI services.

§ 4b Support Access by Authorised Personnel of the Data Processor

4b.1 Under the main contract (§ 8a of the Terms), the Data Processor is entitled to access at any time – without prior individual approval – the Data Controller’s workspaces, configurations and metadata, and, to the extent necessary for the relevant support purpose, content data (in particular posts, media, knowledge stores, brand voices, audiences, channels, log files), in order to fulfil the purposes set out in para. 2.

4b.2 Permitted purposes are exclusively: handling of support requests and incidents; error analysis and reproduction of reported or detected issues; platform security, abuse and incident response; preventive and reactive maintenance and performance optimisation; internal onboarding-related training of authorised persons.

4b.3 To that extent, this DPA constitutes a general documented instruction of the Data Controller pursuant to Art. 28 (3) lit. a GDPR for carrying out the processing operations referred to in para. 2. Processing for the Data Processor’s own purposes remains excluded (§ 3.4).

4b.4 Processing principles:

15. Necessity / need-to-know: access is limited to authorised personnel and to the minimum extent necessary for the purpose.
16. Confidentiality: all accessing persons are bound in writing to confidentiality (cf. § 3.2).
17. Logging: every access is logged with the identity of the accessing person, timestamp, workspace, scope of access and purpose / ticket reference. Logs are retained for at least 12 months and made available to the Data Controller in a suitable format upon a substantiated request.
18. Minimisation: access to content data only occurs where the support purpose cannot be achieved by accessing configuration/metadata alone.

4b.5 Opt-out for sensitive workspaces. The Data Controller may, at any time, mark workspaces or categories of workspaces as sensitive in writing (e-mail is sufficient), thereby activating an extended protection regime. The declaration takes effect upon receipt by the Data Processor. For such workspaces, every support access requires an explicit case-by-case approval by the Data Controller. The Data Controller acknowledges that support, error analysis and security controls for such protected workspaces can only be performed to a limited extent or not at all.

4b.6 Exceptions to opt-out. Irrespective of any opt-out, the Data Processor remains entitled to access a workspace insofar as this is necessary to avert a danger (in particular acute

security incidents, personal-data breaches pursuant to Art. 33 GDPR, prevention of abuse or legal violations) or to comply with statutory obligations. The Data Controller will be informed without undue delay in such cases, unless mandatory legal grounds prevent such notification.

4b.7 Authorised personnel. Support access may only be performed by (a) internal employees of the Data Processor (in particular system administrators, consultants, customer-support staff) who are bound in writing to confidentiality and GDPR compliance, and (b) external freelancers whom the Data Processor has bound by an onboarding agreement to provide customer-support services. The onboarding agreement contains, in particular, confidentiality, data-protection, security and sub-processing clauses (flow-down principle pursuant to Art. 28 (4) GDPR), which are applied to the freelancer as a sub-processor to the extent required. Engagement of any third party outside this group is excluded.

4b.8 The freelancers referred to in para. 7 lit. b are considered sub-processors within the meaning of § 5 of this DPA. They are subject to the provisions of Annex 1 (sub-processor list) to the extent they can be assigned to a category there; in any case, they will be disclosed in writing upon request by the Data Controller. The Data Processor is liable for their fault pursuant to § 5.4.

4b.9 Third-country aspects. Where freelancers have their seat or place of processing outside the EEA, the requirements of § 8 of this DPA additionally apply.

§ 5 Sub-Processing Relationships

5.1 The Data Controller hereby grants general written authorisation for the use of sub-processors listed in Annex 1. The Data Processor is obliged to inform the Data Controller in advance in writing of any intended change with regard to the appointment or replacement of sub-processors.

5.2 The Data Controller may object to an intended change in writing within 14 calendar days of receiving the information. If no objection is raised within this period, the change shall be deemed approved.

5.3 The Data Processor shall ensure contractually that the provisions of this DPA and the data protection obligations also apply to sub-processors used (pass-through principle in accordance with Art. 28 para. 4 GDPR).

5.4 The Data Processor shall be liable to the Data Controller for the negligence of its sub-processors as if it were its own negligence. The liability of the Data Processor for the negligence of sub-processors is limited in amount to the annual net contract value of the main contract. Any liability beyond this is excluded. The limitation of liability does not apply in cases of intent or gross negligence.

5.5 The current list of all sub-processors is attached to this agreement as Annex 1.

5.6 Customer-support freelancers. External freelancers whom the Data Processor has bound by an onboarding agreement to provide customer-support services (§ 4b.7 lit. b) qualify as sub-processors under this section. Insofar as they are not already listed in Annex 1, they will be disclosed in writing upon request by the Data Controller. Otherwise, the provisions of this § 5 apply mutatis mutandis.

Art. 28 para. 4 GDPR

§ 6 Rights and Obligations of the Data Controller

6.1 The Data Controller is responsible for the lawfulness of data processing and ensures that a valid legal basis for processing exists.

6.2 The Data Controller is entitled to verify compliance with this DPA through audits and inspections. Audits shall be conducted with reasonable notice (at least 14 working days) and with due regard for the operational procedures of the Data Processor. Costs incurred by audits and inspections at the Data Processor (in particular personnel costs, documentation costs and preparation) shall be borne by the Data Controller according to actual costs incurred. The agreed hourly rate as per the main contract shall apply, but not less than EUR 150.00 net per hour.

6.3 The Data Processor shall provide the Data Controller with all necessary information to demonstrate compliance with the obligations set out in Art. 28 GDPR and shall permit audits and inspections.

6.4 Instructions from the Data Controller must be given in writing (including email). Oral instructions must be confirmed in writing without undue delay.

Art. 28 GDPR

§ 7 Support Obligations and Data Subject Rights

7.1 The Data Processor shall assist the Data Controller, taking into account the nature of processing, in fulfilling the rights of data subjects under Art. 15-22 GDPR, in particular:

- Right of access (Art. 15 GDPR)
- Right to rectification (Art. 16 GDPR)
- Right to erasure (Art. 17 GDPR)
- Right to restrict processing (Art. 18 GDPR)
- Notification obligation in case of rectification, erasure or restriction (Art. 19 GDPR)
- Right to data portability (Art. 20 GDPR)
- Right to object (Art. 21 GDPR)

7.2 The Data Processor shall further assist the Data Controller with:

- Notification of data breaches to the competent authority (Art. 33 GDPR)
- Notification of data subjects (Art. 34 GDPR)
- Conduct of data protection impact assessments (Art. 35 GDPR)
- Prior consultation with the competent authority (Art. 36 GDPR)

7.3 The support services under § 7.1 and § 7.2 are provided on a fee basis and shall be remunerated according to actual effort at an hourly rate of EUR 150.00 net, provided that the effort has not been caused by a breach of duty by the Data Processor.

Art. 15-22, 33-36 GDPR

§ 8 Third Country Transfers

8.1 Transfer of personal data to third countries outside the EEA is only permitted if the requirements of Art. 44-49 GDPR are met, in particular on the basis of:

- Adequacy decisions by the EU Commission (e.g. EU-US Data Privacy Framework)
- Standard Contractual Clauses (SCCs) in accordance with Art. 46 para. 2 lit. c GDPR
- Binding Corporate Rules in accordance with Art. 47 GDPR
- Supplementary technical and organisational measures in accordance with EDPB recommendations

8.2 Should the Data Processor become aware that a sub-processor is required on the basis of third country law to disclose personal data (e.g. in the context of authority requests under the US CLOUD Act or similar), the Data Processor shall inform the Data Controller without undue delay, to the extent legally permitted. The obligation to provide information is limited to circumstances of which the Data Processor has actual knowledge. There is no independent obligation for the Data Processor to monitor authority requests to its sub-processors.

8.3 The Data Processor generally prefers the use of EU data centres where available. The specific legal bases for third country transfers by the sub-processors used are documented in Annex 1.

Art. 44-49 GDPR

§ 9 Return and Deletion of Data

9.1 After termination of the contractually agreed services, personal data shall initially remain in the Data Processor's system. Deletion or return of data shall only take place on explicit written instruction from the Data Controller.

9.2 If the Data Controller does not issue an explicit deletion or return instruction, the Data Processor is entitled to delete the data after 90 calendar days following contract termination.

9.3 The additional effort associated with data cleaning, return or deletion (in particular for targeted data extraction, format conversion and documented deletion) shall be borne by the Data Controller according to actual effort incurred. The agreed hourly rate as per the main contract shall apply, but not less than EUR 150.00 net per hour.

9.4 Deletion shall be confirmed to the Data Controller in writing upon request.

9.5 Statutory retention obligations (in particular under the Austrian BAO and UGB) remain unaffected. The Data Processor shall inform the Data Controller of such obligations and shall block the affected data for the duration of the retention period.

§ 10 Liability

10.1 The Data Processor's liability for violations of this DPA or the GDPR is limited to a maximum of EUR 10,000.00 per incident or to a maximum of 50% of the respective annual contract sum -- whichever is lower.

10.2 The limitation of liability does not apply in cases of intent, gross negligence or violations of essential data protection core obligations.

10.3 The Data Controller is liable to the extent that it fails to fulfil its own obligations as Data Controller or violates the Data Processor's instructions.

§ 11 Applicable Law and Jurisdiction

11.1 This DPA shall be governed by Austrian law, excluding the UN Sales Convention (CISG) and the conflict of laws provisions of private international law.

11.2 Exclusive place of jurisdiction for all disputes arising out of or in connection with this DPA shall be Linz, Austria.

§ 12 Final Provisions

12.1 Amendments and supplements to this DPA must be made in writing. This also applies to the waiver of the writing requirement itself.

12.2 Should any provision of this DPA be invalid or unenforceable, the validity of the remaining provisions shall remain unaffected. The parties undertake to replace any invalid provision with a valid provision that comes as close as possible to the economic purpose of the invalid provision.

12.3 This DPA is part of the main contract concluded between the parties and takes effect upon its signature.

12.4 In case of conflict between this DPA and the main contract, the provisions of this DPA shall prevail in matters relating to data protection.

Signature Block

[CUSTOMER NAME / COMPANY] -- Data Controller

_____

Place, Date; Name, Function, Signature

All Media FlexCo -- Data Processor

_____

Place, Date; Ing. Mag. Dominik Rockenschaub, Managing Director

Annex 1: Directory of Sub-Processors

The complete and current directory of all sub-processors of All Media FlexCo / ALLMEDIA.AI is maintained in the separate document 'ALLMEDIA_SubAVV_Directory'.

This document contains:

- Complete list of all sub-processors by category
- Location and country of each sub-processor
- Type of service and purpose of processing
- Status of data protection agreements (DPA/Sub-DPA)
- Legal bases for third country transfers

The current status of the sub-processor list shall be provided to the Data Controller upon request or upon material changes in accordance with § 5 of this DPA.

Document Reference: ALLMEDIA_SubAVV_Directory_20260407 (EN) / ALLMEDIA_SubAVV_Liste_20260407 (DE)

Annex 2: Technical and Organisational Measures (TOMs)

The technical and organisational measures in accordance with § 4 of this DPA are documented in the separate document 'ALLMEDIA_TOM'.

The TOM document is an integral part of this DPA and is provided to the Data Controller together with this DPA. The current status shall be made available to the Data Controller upon request or upon material changes.

Document Reference: ALLMEDIA_TOM_EN_20260407 (EN) / ALLMEDIA_TOM_20260407 (DE)

Note: This is the English version of this document. In the event of any discrepancies between the German and English versions, the German version shall prevail.