Data Processing Agreement

Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

This Agreement governs the processing of personal data by BuonaLabs on behalf of a client, as required by Article 28(3) GDPR. It must be signed before any such processing begins.

It supplements the BuonaLabs General Terms of Business and the relevant Project Order. Where it conflicts with them on a data protection matter, this Agreement prevails.

VERSION 1.0 · VALID FROM 15 September 2026 · GOVERNING LAW Federal Republic of Germany

ISSUED BY

BuonaLabs UG (haftungsbeschränkt)
Maria-Goeppert-Straße 3, 23562 Lübeck, Germany
info@buonalabs.com · buonalabs.com
Commercial Register: Amtsgericht Lübeck, HRB 26385 HL
VAT ID: DE455732206
Managing Director: Domingo Buonamassa

PART 1 — AGREEMENT

> *This Agreement is required by Article 28(3) GDPR wherever the Processor processes personal data on behalf of the Controller. It must be concluded before such processing begins. It supplements, and does not replace, the BuonaLabs General Terms of Business.*

Parties

CONTROLLER (CLIENT, LEGAL NAME)	
ADDRESS	
REPRESENTED BY	
DATA PROTECTION CONTACT / EMAIL	
PROCESSOR	BuonaLabs UG (haftungsbeschränkt), Maria-Goeppert-Straße 3, 23562 Lübeck, Germany · HRB 26385 HL
PROCESSOR CONTACT	info@buonalabs.com
RELATED PROJECT ORDER(S)	
EFFECTIVE DATE	

1 Subject Matter, Scope and Duration

1.1 The Processor processes personal data on behalf of the Controller in the course of providing the services described in the Project Order or Project Orders identified above. The subject matter, nature, purpose, duration, types of personal data and categories of data subjects are set out in Annex 1.

1.2 This Agreement applies for as long as the Processor processes personal data on behalf of the Controller and, in respect of obligations that by their nature continue, after that.

1.3 Processing takes place within the European Union or the European Economic Area unless Section 10 applies.

1.4 The Controller is responsible for the lawfulness of the processing, for the legal basis on which personal data are made available to the Processor, and for compliance with its information obligations towards data subjects.

2 Instructions

2.1 The Processor processes personal data only on documented instructions from the Controller, including in respect of transfers to a third country, unless required to do otherwise by Union or Member State law to which the Processor is subject. In that case the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

2.2 The Project Order, this Agreement and its Annexes constitute the Controller's initial documented instructions. Further instructions shall be given in text form to the contact stated above. Instructions given orally shall be confirmed in text form without undue delay.

2.3 The Processor shall inform the Controller without undue delay if, in its opinion, an instruction infringes the GDPR or other applicable data protection law. The Processor may suspend performance of that instruction until the Controller confirms or amends it.

2.4 The Processor shall not use personal data processed on behalf of the Controller for its own purposes, and in particular shall not use them to train, fine-tune or evaluate any machine-learning model, except on the Controller's documented instruction.

3 Confidentiality

3.1 The Processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that the commitment survives the end of their engagement.

3.2 Access is granted only to persons who require it in order to perform the services, and only to the extent required.

4 Security of Processing

4.1 The Processor shall implement the technical and organisational measures required by Article 32 GDPR. The measures in force at the effective date are described in Annex 2.

4.2 The measures are subject to technical development. The Processor may change them provided the level of protection is not reduced. Material changes shall be documented and made available to the Controller on request.

4.3 The Controller has satisfied itself that the measures in Annex 2 are appropriate to the risk of the processing described in Annex 1.

5 Sub-Processors

5.1 The Controller grants the Processor general authorisation to engage sub-processors. The sub-processors engaged at the effective date are listed in Annex 3.

5.2 The Processor shall inform the Controller in text form at least fourteen (14) days before adding or replacing a sub-processor. The Controller may object on reasonable data protection grounds within that period. If the Parties cannot resolve the objection, either Party may terminate the affected Project Order in respect of the affected services, and the Processor is entitled to remuneration for work properly performed to that date.

5.3 The Processor shall impose on each sub-processor, by contract, data protection obligations that are in substance equivalent to those in this Agreement, and remains fully liable to the Controller for the performance of the sub-processor's obligations.

5.4 The use of services that do not involve processing of the Controller's personal data — including ordinary connectivity, compute, monitoring or maintenance where access to personal data cannot be ruled out but is not intended — is not sub-processing for the purposes of this Section, provided appropriate confidentiality and security measures are in place.

6 Assistance with Data Subject Rights

6.1 Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests to exercise rights under Chapter III GDPR.

6.2 If a data subject contacts the Processor directly, the Processor shall not respond on the substance and shall forward the request to the Controller without undue delay.

6.3 Assistance beyond routine effort is remunerated at the Processor's applicable rate, unless the need for assistance arises from a failure attributable to the Processor.

7 Assistance with Articles 32 to 36 GDPR

7.1 The Processor shall assist the Controller, taking into account the nature of processing and the information available to it, in complying with its obligations under Articles 32 to 36 GDPR, including security of processing, breach notification and data protection impact assessments.

7.2 Section 6.3 applies to the remuneration of such assistance.

8 Personal Data Breaches

8.1 The Processor shall notify the Controller without undue delay, and in any event within twenty-four (24) hours, after becoming aware of a personal data breach affecting personal data processed on the Controller's behalf.

8.2 The notification shall describe, as far as known, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Information not available at the time shall be supplied as it becomes available.

8.3 Notification to a supervisory authority or to data subjects is the responsibility of the Controller. The Processor shall not make such a notification on the Controller's behalf unless instructed to do so in text form.

9 Information and Audits

9.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by it.

9.2 Audits shall be announced at least fourteen (14) days in advance, shall take place during normal business hours, shall not unreasonably disrupt operations, and shall be limited to what is necessary. The Controller shall ensure that its auditor is bound to confidentiality and is not a competitor of the Processor.

9.3 The Processor may satisfy an audit request by providing current certifications, approved codes of conduct, or a report by an independent auditor, where these adequately demonstrate compliance.

9.4 Audits beyond one per calendar year, and audits not prompted by a specific incident or by a supervisory authority, are remunerated at the Processor's applicable rate.

10 International Transfers

10.1 The Processor shall not transfer personal data to a country outside the EEA, or to an international organisation, without the Controller's documented instruction and without a valid transfer mechanism under Chapter V GDPR being in place, such as an adequacy decision or the Standard Contractual Clauses together with any supplementary measures required.

10.2 Where a sub-processor in Annex 3 is established outside the EEA, Annex 3 states the transfer mechanism relied upon.

11 Deletion and Return

11.1 On termination of the services, the Processor shall, at the Controller's choice, delete or return all personal data processed on the Controller's behalf, and delete existing copies, unless Union or Member State law requires storage.

11.2 The Controller shall communicate its choice in text form before termination takes effect. In the absence of a choice, the Processor shall delete the personal data thirty (30) days after termination.

11.3 Backup copies are deleted in accordance with the Processor's ordinary backup cycle. Until deletion, they remain subject to this Agreement.

11.4 The Processor shall confirm deletion in text form on request.

12 Liability and Final Provisions

12.1 Article 82 GDPR governs liability towards data subjects. As between the Parties, the liability provisions of the BuonaLabs General Terms of Business apply, subject to mandatory law.

12.2 Where a provision of this Agreement is invalid, the remaining provisions are unaffected. The Parties shall replace an invalid provision with a valid one that most closely reflects its purpose.

12.3 This Agreement is governed by the laws of the Federal Republic of Germany. Mandatory provisions of data protection law remain unaffected.

12.4 In the event of a conflict between this Agreement and the General Terms of Business or a Project Order, this Agreement prevails in respect of data protection matters.

12.5 This Agreement is issued in English. Any translation is for convenience only.

CONTROLLER — CLIENT	PROCESSOR — BUONALABS UG
Name	Name
Title / role	Title / role
Signature	Signature
Place and date	Place and date

ANNEX 1 — DETAILS OF THE PROCESSING

SUBJECT MATTER OF THE PROCESSING	
NATURE AND PURPOSE	
DURATION	
PROCESSING OPERATIONS	

Categories of Data Subjects

Tick or list. Only what the services actually involve.

Types of Personal Data

For example: name, contact details, account and login data, order and payment data, usage and log data, communication content, IP addresses, support tickets.

Special Categories of Personal Data (Article 9 GDPR)

If any special categories are involved, they must be listed here and the Controller must confirm the legal basis. If none, write “none”.

ANNEX 2 — TECHNICAL AND ORGANISATIONAL MEASURES

> *This Annex describes the measures in force. Review it before signing each Agreement and adjust it to what is actually in place — an inaccurate Annex 2 is worse than a short one.*

Confidentiality

- Physical access: work is carried out from secured premises; devices are not left unattended in publicly accessible locations.
- System access: individual accounts, no shared logins, enforced strong passwords held in a password manager, multi-factor authentication on all accounts that support it.
- Data access: access granted on a least-privilege basis and reviewed when a role or engagement ends; production access separated from development access.
- Separation: Controller data are logically separated from the data of other clients and from the Processor's own data.

Integrity

- Transmission: encryption in transit (TLS 1.2 or higher); transfers of files containing personal data by encrypted channel only, never by unencrypted email attachment.
- Storage: full-disk encryption on all endpoints; encryption at rest on managed cloud storage.
- Input control: logging of administrative access and material changes in production systems, with logs retained for an appropriate period.

Availability and Resilience

- Backups according to the schedule agreed in the relevant Project Order, with restore capability tested periodically.
- Patching of operating systems and dependencies on a regular cycle and without undue delay for critical security updates.
- Endpoint protection and firewalling on all devices used to process Controller data.

Procedures for Review and Evaluation

- Data protection management: this Agreement, a record of processing activities, and periodic review of measures.
- Incident response: defined escalation path and notification within the period stated in Section 8.
- Sub-processor control: written agreements, review before engagement, list maintained in Annex 3.
- Privacy by design and by default: data minimisation in system design; test data pseudonymised or synthetic where practicable.
- Instruction control: processing only on documented instruction, with the objection procedure in Section 2.3.

Additional or client-specific measures, where agreed, are recorded in the relevant Project Order and form part of this Annex.

ANNEX 3 — APPROVED SUB-PROCESSORS

List every sub-processor that may process the Controller's personal data, with its role, location and — where outside the EEA — the transfer mechanism relied upon. Keep this current; adding one requires notice under Section 5.2.

SUB-PROCESSOR / SERVICE	PURPOSE	LOCATION	TRANSFER MECHANISM (IF NON-EEA)

CONTROLLER OBJECTION PERIOD 14 days from notice (Section 5.2)

CONTROLLER — CLIENT	PROCESSOR — BUONALABS UG
Name	Name
Title / role	Title / role
Signature	Signature
Place and date	Place and date