DATA PROCESSING AGREEMENT

Between the **Customer**

- Client or main contractor hereinafter referred to as **"Client"**

and **DNAnalytics UG (limited liability**

- Contractor or sub-processor hereinafter referred to as **"Contractor"**

together also "parties"

is agreed:

Preamble

The Contractor shall carry out analyses of coaching sessions conducted and recorded by the Client for the Client using the DNACoachAssist software. In the course of this, personal data from the Client's sphere (in particular Client data) shall be disclosed to the Contractor and the Contractor must process this personal data. In order to be able to carry out this data processing in accordance with applicable data protection law, the parties agree to the following agreement on the processing of data on behalf (hereinafter "DPA").

Depending on the processing situation, the client is either the controller under data protection law or the (first) processor for another controller, i.e. the main contractor. Accordingly, the contractor is either the (first) processor or a sub-processor. The conclusion of this DPA is intended to enable data processing in compliance with data protection law by contractors as the first processor and as sub-processors. With this DPA, the Parties aim to integrate the Contractor into the Client's data processing in compliance with data protection law, regardless of whether the Client is itself the controller or the Contractor is to be integrated into an existing processing chain between the controller under data protection law and the main contractor. All provisions of this DPA must be interpreted in the light of this contractual purpose.

1. **Subject matter and characteristics of commissioned data processing**

1.1. This DPA governs the handling of personal data by the Contractor in the context of the Client's use of DNACoachAssist. Regarding the handling of personal data, the DPA shall take precedence over other contractual provisions and existing confidentiality obligations. Statutory retention obligations of the Contractor shall remain unaffected.

1.2. The subject matter, scope, type and purpose of data processing, the type of personal data and the categories of data subjects are specified in **Annex 1** to this DPA, unless they are already set out in the other contractual provisions. In the event of any contradictions, the provisions of this DPA and all its parts shall take precedence over other contractual provisions

1.3. This agreement also regulates data processing in the subcontracting relationship, if applicable. In order to meet the requirements of data protection law, all rights of the client in accordance with this DPA apply to the respective data controller ("controller"). This also applies without a corresponding explicit reference in the respective clauses.

1.4. The processing and use of data generally takes place in the territory of the Federal Republic of Germany, in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any transfer to a third country only takes place if the specific legal requirements are met.

2. Obligations of the client

2.1. Responsibility for data processing

The client is responsible for the processing and for compliance with the provisions of the data protection laws vis-à-vis third parties, unless the Client itself acts as a processor. The client is responsible for assessing the admissibility of the commissioned processing and the order under data protection law. If the Client is of the opinion that the processing by the Contractor violates the Client's obligations, it must inform the Contractor of this and ensure legally compliant data processing by issuing appropriate instructions.

2.2. Notification and instruction obligations

In the event of a direct request for information, notification, warning or instruction from a supervisory authority pursuant to Art. 58 GDPR, the Client shall support the Contractor. The Client shall ensure that the official request can be complied with in accordance with this DPA.

3. Obligations of the contractor

3.1. Binding to instructions

3.1.1. The Contractor shall process the Client's data exclusively within the scope of this DPA and in accordance with the Client's instructions. This DPA grants the Client a comprehensive right to issue instructions regarding the type, scope and procedure of data processing. This

right to issue instructions is specified by individual instructions. Changes to the object of processing and procedural changes must be jointly agreed and documented.

3.1.2. The Contractor shall only provide information to third parties or the data subjects following prior instruction from the Client. This shall not apply if the Contractor is obliged to disclose such information under applicable law. Section 6.4 remains unaffected.

3.1.3. The Client issues instructions by using the respective functions of the software provided with which the data processing can be controlled (such as the deletion function regarding the transcribed coaching sessions). All instructions outside of these functionalities must be documented and must be issued at least in text form (e.g. by e-mail). The Client shall therefore immediately record any verbal instructions at least in text form. Contractor shall not use the data for any other purposes and is in particular not entitled to pass it on to third parties. No copies or duplicates shall be made without the Client's knowledge. Excluded from this are backup copies, insofar as they are necessary to ensure data processing in accordance with the contract, and copies or duplicates that are necessary to comply with statutory retention obligations.

3.1.4. The Contractor shall inform the Client immediately if he is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to refrain from carrying out such instructions until they have been confirmed or amended by the contact person at the Client. The Contractor does not have to carry out instructions that are obviously unlawful.

3.2. **Data secrecy and obligation of confidentiality**

The Contractor shall ensure that the employees who can access the Client's personal data in accordance with the order or who can otherwise obtain knowledge of the Client's data have been obliged to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality and have been instructed about the special data protection obligations arising from this DPA and the existing instruction or purpose limitation. Other recipients - in particular subcontractors - who may access the Client's personal data in accordance with the order shall be obliged to maintain confidentiality accordingly. The contractor shall ensure that the people who have access to the client's data only process the data in accordance with the client's instructions. Excluded from this are processing operations to which these people are legally obliged.

3.3. **Technical and organizational measures**

3.3.1. Contractor undertakes to maintain appropriate technical and organizational measures to protect the data in accordance with the provisions of Art. 32 GDPR. The technical and organizational measures currently provided are described in **Annex 2**. At the written request of the Client, the Contractor shall disclose the detailed circumstances of the determination, insofar as this does not affect any overriding interests, in particular confidentiality interests, of the Contractor.

3.3.2. The Client is obliged to provide the Contractor with all necessary information that the Contractor requires for an assessment of the technical and organizational measures in accordance with Art. 32 GDPR in good time before the conclusion of the contract and thereafter permanently during the entire term of this DPA. The Client shall immediately and separately point out if special categories of personal data pursuant to Art. 9 GDPR are to be processed (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, health data or data concerning sex life or sexual orientation) or if special features arise for other reasons in the assessment of the processing risk. This applies in particular to an increased likelihood or severity of risk to the rights and freedoms of data subjects.

3.3.3. The technical and organizational measures are subject to technical progress and further development. The Contractor is permitted to implement alternative adequate measures. In doing so, the Contractor shall not fall below the appropriate level of protection. Significant changes must be documented.

4. **Involvement of subcontractors**

4.1. Contractor shall only use subcontractors that he carefully selected, checked and engaged in accordance with section 3.2. The Client gives its general consent to the involvement of subcontractors in the processing or use of personal data. The Contractor shall inform the Client of any intended involvement of a subcontractor. The Client shall have the opportunity to object within 30 days from the date on which the contact person at the Client is informed of the intended involvement by the Contractor. In the event of an objection to the involvement of the subcontractor, the client and contractor shall attempt to find an amicable solution. If no amicable solution is found and if continued data processing by the Contractor without the involvement of the new subcontractor is impossible or objectively unreasonable, the Contractor may terminate

this DPA and the corresponding service contract for good cause. [The subcontractors used are listed in **Annex 1**.]

4.2. The Contractor shall ensure through contractual agreements with the respective subcontractor that the data protection obligations imposed on the subcontractor correspond in the essential points to those of the Contractor under this DPA. This includes appropriate control and inspection rights of the Contractor and the Client to ensure that the technical and organizational measures are implemented in accordance with this DPA. The Client has the right to obtain information from the Contractor in text form on request about the essential contractual content of the subcontracting relationship and the defined list of obligations, if necessary, by inspecting the relevant contractual documents.

4.3. Services that are part of the generally recognized and customary business organization or are of a purely technical nature and whose use is foreseeable for the Client (e.g. telecommunications services, cleaning staff, etc.) are not to be understood as subcontracting relationships within the meaning of this regulation, even if the disclosure of personal data cannot be ruled out in individual cases. The Contractor is equally obliged to take appropriate and reasonable measures to ensure the protection and security of the Client's personal data.

5. **Assistance in responding to data subject rights (rectification, blocking and erasure of data)**

5.1. The protection of data subject rights in accordance with Art. 12 - 22 GDPR is the sole responsibility of the Client. If a data subject contacts the Contractor directly to obtain rectification or erasure of their data or objects to data processing vis-à-vis the Contractor or, in cases of profiling, communicates their own point of view, the Contractor shall forward this request to the Client without delay. The decision on how to deal with this request will be made by the client. The contractor shall only correct, delete or block the data processed on behalf of the client in accordance with the client's instructions. This shall not apply in the case of a corresponding legal obligation and in the case of Section 7.2. The Contractor shall only provide information to the data subject or third parties with the prior consent of the Client.

5.2. Taking into account the nature of the processing and, where possible, with appropriate technical and organizational measures, the Contractor shall support the Client in fulfilling his obligation to respond to requests to exercise the rights of the data subject referred to in Chapter III GDPR.

5.3. The Contractor shall provide personal data to the Client in the format in which it was provided to the Contractor by the Client for processing. The Contractor shall not be obliged to provide the data in any other structured, commonly used and machine-readable format. The Contractor shall

also only disclose the data directly to the data subject or another controller designated by the data subject based on express instructions and only if the Client bears the additional costs incurred in this respect.

6. **Support in complying with reporting obligations in the event of breaches**

6.1. Contractor shall notify Client without undue delay if Contractor becomes aware of a personal data breach. The notice shall include a description of the nature of the personal data breach and, as far as possible, the categories of personal data concerned, and the approximate number of data subjects affected. It is the sole responsibility of the Client to assess the risk resulting from this breach. The contractor shall cooperate in this by notifying the breach and providing the aforementioned information.

6.2. The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 GDPR, taking into account the type of processing and the information available.

6.3. If recommendations of the supervisory authority pursuant to Art. 36 (2) GDPR are to become the basis for processing under this DPA, the Client shall expressly confirm this in writing. This also applies in particular to recommendations made by the supervisory authority directly to the Contractor. The Contractor shall inform the Client of any such recommendations and deadline extensions made directly to the Contractor by the supervisory authority in accordance with Art. 36 (2) GDPR. The Contractor shall only be obliged to implement technical and organizational measures in addition to those taken in accordance with Section 3.3 if the Client assumes the additional costs incurred as a result.

6.4. Contractor shall inform Client about other complaints, inquiries or requests regarding data processing by supervisory authorities or data subjects, in particular about inspection activities, investigations or other measures by supervisory authorities, unless applicable law prohibits such notification due to an important public interest.

6.5. The Contractor shall provide the Client with all necessary information. This also applies to information to defend against third-party claims or with regard to the requirements of supervisory authorities.

7. **Release and deletion of data**

7.1. The Client may at any time during the term of this contract demand the surrender or deletion of the data provided or stored on its behalf. At the end of the respective processing service, the Contractor shall return the data in accordance with the following clauses. The Client shall inform

the Contractor in good time if data is no longer required for processing in accordance with the order. At the end of the respective service contract, the processing service shall in any case be completed as a whole.

7.2. The Contractor shall store the data for a period of 30 days after the end of the order processing agreement. The Client is entitled to demand the surrender or deletion of the stored data at any time until the expiry of this period.

7.3. Documentation that serves as proof of proper data processing in accordance with the order shall be retained by the Contractor beyond the end of the contract in accordance with the respective retention periods. The Contractor may hand them over to the Client for discharge at the end of the contract.

8. **Information and control cooperation obligations**

8.1. Contractor shall cooperate as required, upon reasonable advance notice and appropriate confidentiality agreements, with any assessment, audit or other steps taken for the purpose of verifying that Contractor's processing activities are in compliance with this DPA and applicable law. The Client shall bear all costs of such verification activities, and they shall be conducted in a manner that minimizes disruption to the Contractor's business. To the extent permitted by law, Contractor may provide a summary of the results of a third party audit or certification reports demonstrating compliance with the requirements of the CA Agreement in lieu of the audit measures. Such results and/or the results of such assessments, audits or other steps shall be Contractor's Confidential Information

8.2. Contractor shall provide Client upon reasonable request, no more than once a year, with Contractor's privacy and security policies and other information necessary to demonstrate compliance with the obligations set forth in this DPA.

9. **International data transfers**

Before international data transfer, the Contractor shall ensure that the legal requirements are met, in particular if an international data transfer takes place to a third country in which the level of data protection is below the level of protection within the European Union. To this end, the Contractor implements protection mechanisms. These safeguards may include the Standard Contractual Clauses adopted by the EU Commission on June 4, 2021 (as amended, updated or replaced from time to time) ("EU SCCs") or an adequacy decision issued by the European Commission pursuant to Article 45 GDPR. If the Client itself is located in an unsafe third country (such as the United

States of America), this DPA shall be supplemented by the EU SCCs, which shall become an integral part of this DPA. Module 4 of the EU SCCs applies to the retransfer of data to the Client.

10. **Data Protection Officer**

The Contractor has appointed a data protection officer in writing on the basis of the legal requirements, who can perform his duties properly. This function is performed by the following data protection officer: Paul Matthews (pm@dna-network.de)

11. **Liability**

11.1. The Contractor shall be liable to the Client within the scope of Art. 82 para. 2 sentence 2 GDPR and only if the Contractor culpably breaches an obligation imposed on it by the GDPR or culpably fails to comply with or acts contrary to an instruction lawfully issued by the Client.

11.2. The Contractor shall not be liable if the breach of duty was solely the fault of the Client. In particular, the Contractor shall not be liable to the Client in cases in which the technical and organizational measures agreed with the Client by the Contractor do not meet the requirements of Art. 32 GDPR because the Client does not comply with its information obligations under 3.3.1 or does not comply with them in good time.

11.3. Contractor is liable for the fault of its subcontractors as for its own fault

11.4. Insofar as the Contractor's liability is excluded as a whole or in part in accordance with the above clauses, the Client shall indemnify the Contractor against all claims asserted against the Contractor by third parties due to data processing on behalf of the Client. The same shall apply if a claim by a third party exceeds the amount of fault attributable to the Contractor. The Client is obliged to support the Contractor in an appropriate manner in the defense against the claims raised by third parties and to make all suitable evidence available to the Contractor.

12. **General provisions**

12.1. The amount of the separate remuneration claims for increased expenses under this agreement is set out in the Contractor's price list.

12.2. The term of this DPA is generally unlimited in time. This DPA shall automatically expire when the service relationship between the Client and the Contractor ends.

12.3. The law of the Federal Republic of Germany shall apply to the exclusion of the UN Convention on Contracts for the International Sale of Goods.

12.4. The registered office of the Contractor is agreed as the exclusive place of jurisdiction for all disputes in connection with this GC Agreement, insofar as the Client is a merchant, a legal entity under public law or a special fund under public law.

Annex 1: Order-specific specification of the type and scope of order processing

Annex 2: Technical and organizational measures

Annex 1: Specification of Nature and Scope of Data Processing

No.	Purpose of Processing	Type of Processing	Affected Personal Data	Categories of Data Subjects	Location of Data Processing	Transfer of Personal Data to Sub-processors
1.	Digital management of coaching sessions	Storing, reading, writing, deleting, editing	Name, date of the coaching session, any additional comments from the client, full content of the coaching session	Clients of the Customer	EU (Ireland)	Salesforce Heroku (Website hosting of the software, database via Heroku Postgres)
2.	Uploading recorded coaching sessions as audio files	Storing, reading, writing, deleting, editing	Full content of the coaching session	Clients of the Customer	EU (Frankfurt, Germany)	Amazon Web Services (Temporary storage of audio uploads
3.	Transcription of uploaded audio files	Storing, reading, writing, deleting, editing	Full content of the coaching session	Clients of the Customer	EU and USA	AssemblyAI (AI-based software for transcription
4.	Analysis of transcriptions	Storing, reading, writing, deleting, editing	Full content of the coaching session	Clients of the Customer	EU and USA	Anthropic, PBC (Claude for performing the analyses for US data-residency users)
5.	Analysis of transcriptions	Storing, reading, writing, deleting, editing	Full content of the coaching session	Clients of the Customer	EU	Mistral AI SAS (Mistral models for performing the analyses for EU data-residency users)

Sub-sub-processors of Sub-processors:

Sub-processor	Sub-sub-processor	Purpose
Heroku Salesforce	AWS	As mentioned above under Salesforce Heroku (cf. item 1).

Annex 2

Technical and Organizational Measures of the Contractor

1. CONFIDENTIALITY

Physical Access Control
Technical or organizational measures for access control, especially for authorizing personnel, ensuring that unauthorized persons do not gain access to data processing systems handling personal data:

1.1.1. Telephones, data processing systems, and computers are located in a closed area with restricted access;

1.2. System and Data Access Control

Technical (e.g., password protection) and organizational (e.g., user directory) measures for user identification and authentication to prevent unauthorized access to data processing systems and procedures:

1.2.1. Policies governing the storage of backups.
1.2.2. (Technical) User authentication via password/PIN (minimum length, use of special characters, etc.).
1.2.3. (Technical) Authentication through biometric data.
1.2.4. (Technical) Authentication via chip/key card or mobile device.
1.2.5. (Technical) Use of antivirus software.
1.2.6. (Technical) Mobile device management.
1.2.7. (Technical) Multi-factor authentication (internal/external).
1.2.8. (Technical) Blocking of external interfaces (e.g., USB ports).
1.2.9. (Technical) Logging of data destruction.
1.2.10. (Organizational) Sharing data only with authorized individuals.
1.2.11. (Organizational) User management (only authorized/eligible individuals have basic access).
1.2.12. (Organizational) Password assignment/password policies (length, change intervals, etc.).
1.2.13. (Organizational) Employee training and policies for workflows and access rights to personal data.
1.2.14. (Organizational) Limitation of the number of administrators to the necessary "minimum."
1.2.15. (Organizational) Development of an authorization concept, ensuring data is only accessible to authorized individuals.
1.2.16. (Organizational) Effective and appropriate disciplinary measures against individuals accessing personal data without authorization.

1.3. Data Transmission Control

Measures to ensure personal data cannot be unlawfully read, copied, altered, or removed during electronic transmission, transport, or storage on data carriers, with the ability to retroactively identify where data transmissions occurred:

1.3.1. (Organizational) Strict access restrictions for information identifying the data subjects).
1.3.2. (Organizational) Documentation of data recipients and transmission schedules or agreed deletion periods.
1.3.3. (Organizational) Transfer of data in anonymized or pseudonymized form.
1.3.4. (Organizational) List of procedures
(Organizational) Recording measures

1.4. Pseudonymization

Measures replacing names or identifiers with markers to exclude or significantly hinder the identification of individuals:

1.4.1. (Organizational) Strict access restrictions for information identifying the data subjects.

1.5. Encryption

1.5.1. (Technical) Encryption of (mobile) storage devices/removable media.
1.5.2. (Technical) Access only via secure/encrypted connection.
1.5.3. (Technical) Encryption of storage media according to industry standards.
1.5.4. (Technical) Email encryption.
1.5.5. (Technical) Encrypted storage compliant with applicable industry standards.

2. INTEGRITY

2.1. Input / Input Control

Measures ensuring that subsequent verification can establish whether, and by whom, personal data was entered, altered, or deleted in data processing systems:

2.1.1. Measures to protect against unauthorized alteration and/or deletion of stored data.
2.1.2. (Technical) Recording of data entry, modification, and deletion.
2.1.3. (Technical) User identification following access control protocols.
2.1.4. (Technical) Logging of access to applications, especially during data entry, modification, and deletion.
2.1.5. (Organizational) Preparation of an overview of applications where data entry, modification, and deletion occur.
2.1.6. (Organizational) Transparency in data entry, modification, and deletion through individual usernames (no group usernames).
2.1.7. (Organizational) Granting rights to enter, modify, and delete data based on an authorization concept. (Technisch) - Aufzeichnung der Eingabe, Änderung und Löschung von Daten.

2.2. Integrity Control (Detection of Integrity Violations)

2.2.1. (Technical) Regular integrity checks of data.
2.2.2. (Technical) Real-time detection of integrity violations.

3. AVAILABILTY AND RELIABILITY

3.1. Availability Control

Physical/logical data security measures ensuring that personal data is protected against accidental destruction or loss:

3.1.1. (Technical) Policies prohibiting the storage of personal data on local storage devices.
3.1.2. (Technical) Infrastructure redundancy (e.g., load balancing, RAID).
3.1.3. (Technical) Antivirus concepts/malware protection/IDS/IPS.
3.1.4. (Technical/Organizational) Regular data backups following a backup and recovery concept.
3.1.5. (Organizational) Effective emergency plan.
3.1.6. (Organizational) Proactive monitoring of resources for bottlenecks or potential failures.

3.2. Stress Control

Measures ensuring the smooth functioning of data processing systems even under stress:

3.2.1. (Technical) Continuous performance monitoring and proactive mitigation of bottlenecks.
3.2.2. (Organizational) Performance testing during development and changes.

3.3. Recoverability Control

3.3.1. (Organizational) Regular verification of backup restorations.

4. PROCESS CONTROLL AND SECURITY CONCEPT EVALUATION

4.1. Contract/Order Control

4.1.1. Access controls as described under System and Data Access Control.
4.1.2. (Organizational) Regular validation of access rights.
4.1.3. (Organizational) Clear written instructions to the data processor on the scope of personal data processing.
4.1.4. (Organizational) Ensuring data destruction upon contract termination.
4.1.5. (Organizational) Ensuring compliance with data protection regulations by the processor's personnel.
4.1.6. (Organizational) Pre-assessment of security measures implemented by the processor and related documentation.

4.2. Separation Control

Measures ensuring that data collected for different purposes is processed separately:

4.2.1. (Technical) Modules in the contractor's database distinguishing various purposes of data use, e.g., differentiation by functionality and role.
4.2.2. (Technical) Configuration of interfaces, batch processing, and reports for specific purposes and functions, ensuring separate processing of data collected for different purposes.
4.2.3. (Technical) Physical separation of storage on separate systems or media.
4.2.4. (Technical) Separation of production and test systems.
4.2.5. (Technical) Security measures ensuring only authorized users access data.
4.2.6. (Technical) Logical client separation (software side).
4.2.7. (Organizational) Development of an authorization concept.
4.2.8. (Organizational) Provision of datasets with purpose attributes/data fields.

4.3. Retention/Deletion Control

4.3.1. (Organizational) Sample checks of deletions or settings.

4.4. Default Protection

4.4.1. (Organizational) Review of implementation requirements.
4.4.2. (Organizational) Review of implementation requirements.

4.5. Data Protection Management / Effectiveness Reviews / Certificates

4.5.1. (Organizational) Regular provision of security/data protection certificates.
4.5.2. (Organizational) Regular review of the supplier.