Processing Agreement

in accordance with Article 28 General Data Protection Regulation (GDPR)

between

Customer

(the Controller – hereinafter referred to as the Client)

and

STABILO International GmbH
Schwanweg 1
90562 Heroldsberg
(the Processor - hereinafter referred to as the Supplier)

Sec. 1 Subject matter and duration of the Order or Contract

1. Subject matter
The Subject matter of the Order or Contract regarding the processing of data is the execution of the following services or tasks by the Supplier: *Storage of the customer's encrypted Handwriting-Donation App data for the purpose of improving AI handwriting recognition models.*

2. Duration

The duration of this Order or Contract corresponds to the duration of the Service Agreement.

Sec. 2 Specification of the Order or Contract Details

Detailed description of the Subject Matter with regard to the Nature and Purpose of the services provided by the Supplier: Appendix 1, Point A.

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

The type of personal data used is precisely defined in the Service Agreement under: **Appendix 1, Point B.**

The Categories of Data Subjects are precisely defined in the Service Agreement under: Appendix 1, Point C.

Sec. 3 Technical and Organisational Measures

1. Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and

shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

2. The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in Appendix 2].

3. The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

Sec. 4 Rectification, restriction and erasure of data

1. The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

2. Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

Sec. 5 Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

1. Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR.

> His/Her current contact details are always available and easily accessible on the website of the Supplier.

2. Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so otherwise by law.

3. Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Appendix 1].

4. The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

5. The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.

6. Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.

7. Verifiability of the Technical and Organisational Measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

Sec. 6 Subcontracting

1. Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

2. The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company subcontractor	Address/country	Service
Telekom Deutschland GmbH	Landgrabenweg 151, 53227 Bonn	Hosting of the data on Telekom servers

Outsourcing to subcontractors or Changing the existing subcontractor are permissible when:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

An objection to the planned outsourcing may mean that the service may not take place.

3. The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

4. If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

5. Further outsourcing by the subcontractor **r**equires the express consent of the main Client (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

Sec. 7 Supervisory powers of the Client

1. The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

2. The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR**.** The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

3. The Supplier may claim remuneration for enabling Client inspections.

Sec. 8 Communication in the case of infringements by the Supplier

1. The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
b) The obligation to report a personal data breach immediately to the Client
c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
d) Supporting the Client with its data protection impact assessment
e) Supporting the Client with regard to prior consultation of the supervisory authority

2. The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

Sec. 9 Authority of the Client to issue instructions

1. The Client shall immediately confirm oral instructions (at the minimum in text form).

2. The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

Sec. 10 Deletion and return of personal data

1. Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

2. After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

3. Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

Appendix 1: A. Additions to Sec. 2 Nature and Purpose of the services provided by the Supplier
B. Additions to Sec. 2 Type of personal data
C. Additions to Sec. 2 Categories of Data Subject

Appendix 2: Technical and Organisational Measures pursuant to Art. 32 GDPR

Appendix 1:

A. Additions to Sec. 2 scale, manner and purpose of data processing

Storage of the app data in the cloud to enable improvement of handwriting recognition algorithms. The data are access-protected.
Definition of the contract duration: As long as the client actively uses the app, the contract is active. If there is no active use for more than 24 months, the contractor reserves the right to delete the data irrevocably. By specifying the backup ID, the client has the option to have the data deleted from the server by the contractor at any time.

B. Kinds of data according to Sec. 2

User data (username/ID (if applicable), writing position (if applicable), handedness, optionally gender, language, year of birth, school year (if applicable)), DigiPen sensor data (raw) and (if applicable) WACOM trajectory data during recording, as well as (optionally) a photo of the writing

C. Persons affected according to Sec. 2

Every app user

Appendix 2: Technical and Organisational Measures pursuant to Art. 32 GDPR

Documentation of technical and organisational measures according to Art. 32 GDPR[1].

1.	**Pseudonymisation*** Which measures are taken to guarantee pseudonymisation of personal data? Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	No names or exact birth dates that allow identification are being stored
2.	**Encryption*** Which measures are taken to guarantee encryption of personal data? Measures of encryption transform a clear text depending on an item of additional information (known as the key) into a corresponding secret text (cipher text or enciphered text), which should not be decryptable for anyone not in possession of the key.	use of cryptographic tools
3.	**Ability to ensure confidentiality*** Which measures are taken to permanently guarantee the ability of confidentiality of the data? Confidentiality means that personal data is protected against unauthorised disclosure.	individual log-ins and password procedures encryption of systems encryption of communication

[1] This Document serves the purpose of fulfilling legal obligations and aims to provide a general description which allows a provisional assessment on the adequacy of the adopted data security measures. Within the duration of the contract, this data security concept shall be adapted and updated to current circumstances. All updates and changes to the contract implementation shall be documented in written form. This document is part of the contract and shall be submitted to the Controller yearly and in event of significant changes.

4.	**Ability to ensure integrity*** Which measures are taken to permanently guarantee the ability of integrity of the data? Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is used in connection with the term "data", it expresses that the data is complete and unchanged.	use of access rights loggings within the system
5.	**Ability to ensure availability*** Which measures are taken to permanently guarantee the ability of availability of the data? The availability of services and IT systems, IT applications, and IT network functions or of information is guaranteed, if the users are able to use them at all times as intended.	back-up procedures mirroring hard drives perpetual electric power supply antivirus protection / firewall
6.	**Ability to ensure resilience*** Which measures are taken to permanently guarantee the ability of resilience of the data? Systems are resilient when they are so resistant that their functionality is given even in case of strong access or heavy load.	penetration testing
7.	**Restoration*** Which measures are taken to guarantee that personal data is available and accessible in a timely manner in the event of a security incident?	back-up procedures perpetual electric power supply
8.	**Process for regularly testing*** How is it ensured that the data security measures are reviewed regularly?	predetermined test routine exists
9.	**Unauthorised access to personal data** Which measures are taken to prevent that personal data is available and accessible to unauthorized persons?	individual log-ins and password procedures additional log-ins for certain applications documentation of permissions
10.	**Instruction of employees** How do you ensure that personal data are only processed in accordance with the instructions from the controller?	engagement of employees to codes of conduct implementation of internal privacy policies