Commissioned data processing agreement in conformity with Art. 28 GDPR

by and between

Data controller / You / user of IDLaS (subsequently referred to as the controller)

and

Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. (subsequently referred to as „MPG“)

Represented by the Managing Director Prof. Dr. Antje Meyer
acting on behalf of the

Max Planck Institute for Psycholinguistics
Wundtlaan1
6525XD Nijmegen
The Netherlands

- subsequently referred to as „**MPI**“-
- commissioned processor -
- subsequently referred to as the processor -

Section 1 Subject Matter and Duration of Commission

The processor makes available a collection of 36 behavioural tests suited to assess individual differences in language skills. The tests have been piloted in individuals aged between 18 and 30. The tests require participants to provide spoken and written responses, as well as (speeded) button presses. The processor provides an online platform for controllers to run the tests remotely (i.e., via the internet). Controllers may create customized versions of the test battery by including/excluding tests of their choice, in the order of preference and dividing tests into sessions of variable length. A session-test configuration is labelled ‘a study’, associated with a unique identifier (‘study key’) and stored. The Controllers can manage studies associated with the provided email address and identifier (‘researcher key’). Managing includes revising and deleting a session-test configuration. The processor also makes available the ‘Electron program’, wherein the tests can be run. Electron is an emulation of the Chrome browser. Finally, the processor provides a ‘data retrieval’ service, which includes a set of R scripts that retrieve and aggregate the collected data associated with a provided study key.

In its initial phase, the IDLaS-NL service and technical support will be available until 31.05.2026.

Within the scope of using our service, the data collected and uploaded to our server will be stored and made available to the controller who used the service.

The processor shall perform the agreed services only as defined in the relevant agreements and in accordance with the subject matter and duration of the commission.

Section 2 Scope, Type and Purpose of the Intended Data Processing

(1) Within the scope of the commission, the processor shall process the following personal data: *Email address, audio (voice) recordings, age, gender, educational background, mother tongue*
The personal data relate to the following groups of individuals:
- E-Mail address: Controller
- Age, gender, educational background, mother tongue, medical issues: Any test taker of the IDLaS battery
- Audio (voice) recordings: Any test taker carrying out a language production test of the IDLaS battery

(2) Data processing shall be performed for the following purposes only: *To make use of our service/tool. The processor reserves the right to use the collected data for academic purposes, including – but not limited to – statistical analyses and the publication of scientific articles.*

(3) According to the controller's Security Levels Concept, the data are classified in the following protection categories:
☐ normal
X high
☐ very high

(4) The processor may only collect, process or use the personal data within the scope of the documented instructions given by the controller. The processor shall be bound by the controller's instructions throughout the life of the contract.

(5) Pursuant to this Agreement, all contractual data may only be processed and stored in countries which are members of the European Union or signatory states to the Agreement on the European Economic Area. The processor hereby gives their assurance that they will protect the contractual data against access by governmental entities outside the European Union or the European Economic Area.

(6) Any transfer of personal data to a third country requires the controller's prior approval and shall only take place if the special conditions laid down in Art. 44 ff. General Data Protection Regu-

lation (GDPR) are complied with. These shall be specified separately.

(7) The processor shall refrain from using data which are disclosed to them during or in the context of fulfilment of the contract for purposes other than those stipulated. Copies or duplicates must not be made unless the controller is aware of this and has given prior written permission. Exception: backup copies which are made so that data processing can be performed properly and so that liability and warranty claims can be fulfilled.

(8) The processor may not provide information to third parties, including data protection supervisory authorities, without consulting the controller first.

Section 3 Controller's Rights and Duties

(1) The controller is the data controller (§ 4, para. 7 GDPR) for commissioned data processing carried out by the processor. Assessment of the legality of the data processing is in the controller's responsibility.

(2) The controller shall be responsible for upholding the rights of the parties involved. The processor must immediately notify the controller if parties involved assert their rights vis-a-vis the controller.

(3) The controller shall instruct the processor to comply with all obligations under this Agreement. The controller shall be entitled to issue additional instructions to the processor at any time regarding the type, scope and nature of data processing. Instructions may be issued in writing or via email bearing a digital signature.

Section 4 Processor's Rights and Duties

(1) The processor regularly controls data processing and internal processes and immediately informs the controller in case of suspected violation of the protection of personal data, cases of serious operational disruptions or other irregularities in the processing of the controller's data. The processor shall take the necessary measures to secure the data and to mitigate possible adverse consequences of the persons concerned and shall consult with the controller without delay. The processor shall immediately provide the controller with all the information requested, in particular the information required for the reporting in ac-

cordance with Articles 33, 34 GDPR and shall assist it in the fulfilment of the controller's obligations under Articles 33, 34 GDPR. The processor shall allow the controller or third parties designated by the controller without delay to carry out their own investigations of data processing.

(2) The processor shall immediately inform the controller if the processor deems an instruction to be in violation of the GDPR or other data protection provisions of the EU or the member states.

(3) The processor shall notify the controller before announced inspections by the data protection authorities if contractually agreed services will be affected or if the data protection authorities' inspection might have consequences for the type and manner of contractual fulfilment. The processor shall also notify the controller if an authority investigates the processing of personal data by the processor in the course of criminal proceedings or proceedings for fines or if investigations for other reasons are carried out in connection with such data on the part of the processor.

(4) Furthermore, when first requested to do so, the processor shall immediately and comprehensively supply the controller with all necessary information regarding the collection, storage, processing or transfer of personal data which may be needed to fulfil any duties to provide information vis-a-vis parties involved or the relevant authorities. The processor shall assist the controller in the fulfilment of their obligations under Articles 35 and 36 GDPR (data protection impact assessment and prior consultation) and shall provide all information necessary for this purpose.

(5) The processor shall support the controller to the best of their ability in proceedings before the supervisory authority, in fine, criminal or administrative proceedings, in disputes with affected parties or third parties in connection with commissioned processing or personal data, in particular in the event of a claim for possible claims pursuant to Article 82 GDPR. As far as these activities exceed the contractually agreed scope of services, the processor can demand an appropriate remuneration.

(6) The support services set out in paragraph 1 to 5 are provided by the processor free of charge insofar as is reasonable and appropriate.

(7) Correction, deletion or blocking of personal data shall only be performed by the processor upon appropriate instruction and/or prior approval from the controller. The processor must set up their infrastructure in such a way and take all other measures

necessary so that they can immediately fulfil such requirements issued by the controller. Within the scope of the processor's possibilities and within the scope of the instructions of the controller, the processor supports the controller in fulfilling the inquiries and claims of persons concerned in accordance with Chapter III of the GDPR.

(8) The processor assures that they have appointed a competent and reliable data protection officer who is granted the necessary time to carry out their tasks in accordance with Articles 38 and 39 GDPR. The processor provides the controller with the data protection officer's contact details without delay. This applies also in the event that a new data protection officer takes office. If the processor is not obliged to appoint a data protection officer, they shall inform the controller accordingly.

§ 5 Commitment to Data Confidentiality

(1) The processor guarantees that the employees involved in processing the data of the principal and other persons working for the processor are prohibited from processing the data outside the instructions of the controller. Furthermore, the processor guarantees that the persons authorized to process the personal data have undertaken to maintain confidentiality or are subject to an appropriate statutory commitment to non-disclosure. The commitment to confidentiality/non-disclosure shall continue to apply even after termination of the commission.

(2) The processor hereby gives their assurance that they have made the staff assigned to the commission familiar with the data protection legislation relevant to them. The processor shall monitor compliance with data protection legislation and with the instructions given.

Section 6 Technical and Organizational Measures

(1) The processor shall design the internal organization within their area of responsibility in such a way that it meets the special requirements of data protection. They will take technical and organizational measures to adequately protect the controller's data in order to ensure a protection level appropriate to the risk, based on the level of data protection specified by the client.

(2) The technical and organizational measures must meet the requirements of the GDPR (Art. 32 GDPR) and ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing in the long term. The state of technology, the implementation costs and the type,

scope, circumstances and purposes of the processing as well as the probability of occurrence and severity of the risk to the rights and freedoms of natural persons, in particular through possible violations of the protection of personal data pursuant to Art. 32, para. 2 GDPR, must be taken into account.

(3) The technical and organizational measures to be undertaken by the processor are available upon request. Please send an email to privacy@mpi.nl, topic “TOM’s IDLAS” to receive the most recent version.

(4) The processor shall use a procedure pursuant to Art., 32 para. 1 d) GDPR for the regular review of the effectiveness of the technical and organizational measures to ensure the safety of the processing and shall inform the controller of the results of the review.

(5) During the course of the commission relationship, technical and organizational measures may be modified as part of ongoing technical and organizational changes. Any changes must be set forth in writing.

(6) Personal or sensitive data may only be transmitted via encrypted connections or in an encrypted form. If the recipient requires a password or other form of key for decryption, this must be transmitted by a different method than the connection to be encrypted. The processor shall bear any costs incurred by them for the encryption.

(7) Secure communication by e-mail must be carried out using end-to-end encryption. If special categories of personal data within the meaning of Article 9 GDPR and confidential data is communicated by e-mail, S/MIME is to be used. For this purpose, the processor shall ensure during the entire term of the contract that its employees have S/MIME-capable mail clients with signature and encryption function as well as valid certificates which comply with the minimum requirements of the “Notice on electronic signatures according to the Signature Act and the Signature Ordinance (overview of suitable algorithms)” and which are issued by a common certification authority. Outgoing e-mails sent by the processor's employees must be digitally signed as standard. If the recipient requires a password or other form of key for decryption, this must be transmitted by a different method than the connection to be encrypted. The processor shall bear any of its own costs incurred by the encryption.

(8) Personal or sensitive data must be transmitted via encrypted connections or in encrypted form only. If the recipient requires a password or other form of key material for decryption, this must

be transmitted through a different channel than the connection to be encrypted. The contractor shall bear the costs of encryption incurred on their part.

(9) Email messages between the parties regarding data protection, secrecy and security will only be accepted if a digital signature is added to the text part of the email. In the case of personal or sensitive content, the message must also be encrypted.

(10) The processor advises and supports the client in the selection and implementation of the suitable technical and organizational measures in order to effectively implement the data protection principles contained in the GDPR (e.g. data minimization), to incorporate the necessary guarantees into the processing in order to meet the requirements of the regulation and to protect the rights of the persons concerned (privacy by design). The same applies to technical and organizational measures to ensure that only such personal data the processing of which is necessary for the respective specific processing purpose is processed (privacy by default).

Section 7 Controller's Rights and Duties

(1) The processor shall provide the controller with proof of compliance with the obligations laid down in this contract by suitable means.

(2) The controller shall have the right to carry out checks in consultation with the processor or to have them carried out by auditors to be named in individual cases, the costs of which shall be borne by the controller. The controller has the right to convince themselves of the processor's compliance with this contract in the processor's business operations by means of spot checks, which as a rule must be notified in good time.

(3) The processor shall ensure that the controller can satisfy themselves of the processor's compliance with the obligations under Art. 28 GDPR. The processor undertakes to provide the controller with the necessary information on request and in particular to provide evidence of the implementation of the technical and organizational measures.

(4) The processor shall also be able to provide the following evidence:

- Certification according to an approved certification procedure in accordance with Art. 42 GDPR;
- Current certificates, reports or extracts from reports from independent bodies (e.g. auditors, auditors, data protection officer, IT security department, data protection auditors, quality auditors);

- suitable certification through IT security or data protection audits (e.g. according to BSI Grundschutz (German Federal Office for Information Security – Basic Protection);

The controller's rights in accordance with paragraphs 2 and 3 to carry out inspections and to demand information remain unaffected.

(5) The costs incurred on their side shall be borne by the contracting parties themselves.

Section 8 Subcontracting

(Intentionally left open)

Section 9 Surrender, Deletion, End of Contract

(1) After complete performance of the contract or upon the controller's request also earlier than that, but at the latest upon termination of the commission, the contractor shall hand over the controller's data as well as the other data stocks in connection with the contractual relationship, all documents obtained by the processor as well as processing and usage results produced shall be handed over to the controller or destroyed in conformity with data protection regulations in accordance with the latter's written instructions. The same applies for test materials and discarded materials. Upon request, the report of deletion or destruction shall be submitted.

(2) However, backup copies which have been made in order to fulfil liability and warranty claims shall remain unaffected. The processor shall keep these items safe for the controller until they are fully surrendered to the controller and must surrender them to the controller when first asked to do so. The processor shall secure these items against damage or loss in an appropriate manner, in particular by storing and archiving them properly. Backup copies must be locked using suitable methods in order to ensure that the processor cannot use them. The processor shall provide the customer with information on such back-up copies at any time.

(3) Documents and files which are no longer required must not be destroyed until prior written permission has been given by the controller in accordance with the relevant data protection legislation, providing appropriate evidence.

(4) Documentation that serves as proof of commissioned processing as well as compliant data processing must be kept by the processor after the end of the contract in accordance with the re-

spective retention periods. At the end of the contract, the controller may hand the documentation over to the controller for their discharge.

Section 10 Liability

(1) The parties are liable to third parties in accordance with Art. 82 GDPR.

(2) The internal compensation between controller and processor is based on Art. 82, para. 5 GDPR.

(3) For fines imposed on one of the parties due to an infringement under Article 83 GDPR, the parties are also liable in internal settlement in accordance with Article 82 para. 5 GDPR.

Section 11 Termination

Each infringement against the provisions of this Agreement shall constitute grounds for extraordinary termination.

Section 12 Final Provisions

(1) If data of the controller which are held by the processor are jeopardized due to the action of a third party (e.g. execution or seizure), insolvency or settlement proceedings or other events, the processor must immediately notify the controller. The processor must also inform the third party that the data are the controller's data and that the processor processes the data only on behalf of the controller.

(2) There shall be no retention rights per § 273 Civil Code *(Bürgerliches Gesetzbuch – BGB)* with regard to the processed data or accompanying data media.

(3) In the event case of contradictions to other contract terms, the provisions of this Agreement have priority.

(4) Amendments and supplements to this contract and all its components – including any assurances of the contractor – require a written agreement, which can also be made in electronic form, and an express indication that these conditions are to be amended or supplemented. This also applies to the waiver of this form requirement.

(5) If a provision of this Agreement is invalid, the validity of the other provisions shall remain unaffected. If a provision proves invalid, the parties shall replace it with a new provision which approximates as closely as possible to what the parties intended.

(6) German law applies.

_____	_____
Date /	Date/
Controller signature	Processor signature