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.

Only the German version of this agreement is authoritative.

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, native language, handedness, medical issues
  The personal data relate to the following groups of individuals:
  Controller: E-Mail address
  Any test taker of the IDLaS battery: Age, gender, educational background, mother tongue, medical issues
  Any test taker carrying out a language production test of the IDLaS battery: Audio (voice) recordings

(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:

X 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 Regulation (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 accordance 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 pur-

suant 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.

Section 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) 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).

(6) 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

(7) 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. 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. The processor shall bear any costs incurred by them for the encryption.

(8) 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.

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 respective 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

(1) 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

VERTRAG ZUR AUFTRAGSVERARBEITUNG GEMÄß ART. 28 DS-GVO

von und zwischen

Auftraggeber (Data controller)/You/ IDLaS Nutzer*in

– nachfolgend „**Verantwortlicher**“ genannt –

und

Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.
(eingetragen im Vereinsregister zu Berlin)

– nachfolgend „**MPG**“ genannt –

hier vertreten durch die Geschäftsführende Direktorin Prof. Dr. Antje Meyer
handelnd für das

Max-Planck-Institut für Psycholinguistik
Wundtlaan1
6525XD Nijmegen
Niederlande

– nachfolgend „**MPI**“ genannt –
– MPG und MPI gemeinsam nachfolgend „**Auftragsverarbeiterin**“ genannt –
– Auftraggeber und Auftragnehmer gemeinsam nachfolgend „**Vertragspartner**“ genannt –

wird folgender Vertrag (im Folgenden: „**Vereinbarung**“) geschlossen:

§1 Gegenstand des Auftrags

Die Auftragsverarbeiterin stellt 36 Verhaltenstests zur Verfügung, mit denen individuelle Unterschiede in Sprachfähigkeiten gemessen werden können. Die Tests wurden bei Personen im Alter zwischen 18 und 30 Jahren pilotiert und normiert. Die Tests erfassen mündliche und schriftliche Antworten von den Teilnehmenden sowie das (schnelle) Drücken von Tasten. Die Auftragsverarbeiterin stellt den Verantwortlichen eine Online-Plattform zur Verfügung, um die Tests über das Internet durchzuführen. Die Verantwortlichen können angepasste Versionen der Testbatterie erstellen, indem sie die gewünschten Tests auswählen. Ebenfalls kann die Reihenfolge der Tests nach Belieben geändert und können die Tests über mehrere Sessions verteilt werden. Eine solche Konfiguration wird als „Studie“ bezeichnet und ist mit einer eindeutigen Kennung („Studienschlüssel“) versehen. Die Verantwortlichen geben eine E-Mailadresse an, welche an eine Studie gekoppelt wird. Zudem wird ein „Forscher*innenschlüssel“ generiert, der ebenfalls an die Studie gekoppelt wird. Beide Schlüssel und die E-Mailadresse werden zur Verwaltung einer Studie benötigt. Die Verwaltung umfasst das Überarbeiten und Löschen einer Konfiguration. Weiterhin stellt die Auftragsverarbeiterin ein „Elektronprogramm“ zur Verfügung. Electron ist eine Emulation des Chrome-Browsers. Studienteilnehmende sollen die Tests in diesem Programm ausführen. Die Auftragsverarbeiterin stellt zudem einen „Datenabruf-Dienst“ bereit, der eine Reihe von R-Skripten umfasst, die die mit einem Studienschlüssel assoziierten Daten abruft, aggregiert, und per E-Mail zum Download zur Verfügung stellt.

In der Anfangsphase wird der Service und technische Support von IDLaS-NL bis zum 31.05.2026 verfügbar sein.

Im Rahmen der Nutzung des Dienstes werden die erhobenen und auf unseren Server hochgeladenen Daten gespeichert und den Verantwortlichen, der den Dienst genutzt hat, zur Verfügung gestellt. Die Auftragsverarbeiterin führt die vereinbarte Leistung ausschließlich im Rahmen der getroffenen Vereinbarungen nach dem Gegenstand und der Dauer des Auftrags durch.

Allein die deutsche Version dieses Vertrages ist maßgebend.

§2 Umfang, Art und Zweck der vorgesehenen Datenverarbeitung

(1) Die Auftragsverarbeiterin verarbeitet im Rahmen des Auftrags folgende Arten personenbezogener Daten:

- E-Mailadresse, Stimmenaufnahmen, Alter, Geschlecht, Bildungsstand, Muttersprache, Händigkeit, medizinische Probleme

  Die persönlichen Daten werden für die folgenden Personengruppen erhoben:

  Verantwortliche: E-Mailadresse

  Studienteilnehmende: Alter, Geschlecht, Bildungsstand, Muttersprache, Händigkeit, medizinische Probleme

  Studienteilnehmende, die an einem Experiment zur Sprachproduktion teilnehmen: Stimmenaufnahmen

(2) Die Datenverarbeitung erfolgt ausschließlich zu folgenden Zwecken:

- Zur Nutzung des Dienstes. Die Auftragsverarbeiterin behält sich das Recht vor, die gesammelten Daten für akademische Zwecke zu verwenden, einschließlich – aber nicht beschränkt auf – statistische Analysen und die Veröffentlichung wissenschaftlicher Artikel.

(3) Die Daten werden entsprechend dem Schutzstufenkonzept des Verantwortlichen in folgende Kategorien eingeordnet:

- **hoch**

(4) Die Auftragsverarbeiterin darf die personenbezogenen Daten nur im Rahmen der dokumentierten Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. Die Auftragsverarbeiterin ist während der gesamten Laufzeit des Vertrages an die Weisungen des Verantwortlichen gebunden.

(5) Sämtliche vertragsgegenständlichen Daten dürfen nur in Staaten, die Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, verarbeitet und gespeichert werden. Die Auftragnehmerin sichert zu, die vertragsgegenständlichen Daten vor einem Zugriff staatlicher Stellen außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums zu schützen.

(6) Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Diese sind gesondert festzulegen.

(7) Die Auftragsverarbeiterin verwendet Daten, die ihr im Rahmen der vertraglichen Erfüllung oder im Zusammenhang damit bekannt geworden sind, nur für die vorgesehenen Zwecke. Kopien oder Duplikate dürfen ohne Wissen und schriftlicher Zustimmung des Verantwortlichen nicht erstellt werden. Hiervon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung, sowie zur Erfüllung von Haftungs- und Gewährleistungsansprüchen.

(8) Auskünfte an Dritte, auch an Datenschutzaufsichtsbehörden, darf die Auftragsverarbeiterin nicht ohne vorherige Konsultation des Verantwortlichen erteilen.

§3 Rechte und Pflichten des Verantwortlichen

(1) Der Verantwortliche ist „Verantwortlicher" im Sinne des Art. 4 Ziff. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch die Auftragsverarbeiterin. Die Beurteilung der Rechtmäßigkeit der Datenverarbeitung obliegt dem Verantwortlichen.

(2) Der Verantwortliche ist für die Wahrung der Betroffenenrechte verantwortlich. Die Auftragsverarbeiterin wird den Verantwortlichen unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber der Auftragsverarbeiterin geltend machen.

(3) Der Verantwortliche erteilt der Auftragsverarbeiterin die Anweisung, sämtliche Pflichten nach diesem Vertrag einzuhalten. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können schriftlich oder per digital signierter E-Mail erfolgen.

§4 Rechte und Pflichten des/der Auftragsverarbeiterin

(1) Die Auftragsverarbeiterin kontrolliert regelmäßig die Datenverarbeitung und die internen Prozesse und informiert den Verantwortlichen unverzüglich bei Verdacht der Verletzung des Schutzes personenbezogener Daten, über Fälle von schwerwiegenden Betriebsstörungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Die Auftragsverarbeiterin trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Verantwortlichen ab. Die Auftragsverarbeiterin erteilt dem Verantwortlichen unverzüglich alle verlangten Auskünfte, insbesondere die für die Meldungen nach Artikel 33, 34 DS-GVO erforderlichen Informationen, und unterstützt ihn bei der Erfüllung seiner Pflichten nach Artikel 33, 34 DS-GVO. Die Auftragsverarbeiterin gestattet dem Verantwortlichen oder von ihm benannten Dritten unverzüglich eigene Untersuchungen der Datenverarbeitung.

(2) Die Auftragsverarbeiterin informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die Datenschutz-Grundverordnung oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedsstaaten verstößt.

(3) Die Auftragsverarbeiterin benachrichtigt den Verantwortlichen, bevor eine angekündigte Kontrolle einer Datenschutzaufsichtsbehörde stattfindet, sofern vertraglich geschuldete Leistungen hiervon betroffen sind oder sich aus der Überprüfung der Aufsichtsbehörde Konsequenzen für die Art und Weise der Vertragserfüllung ergeben können. Die Auftragsverarbeiterin benachrichtigt den Verantwortlichen auch, soweit eine Behörde im Rahmen eines Strafverfahrens-, oder Bußgeldverfahrens in Bezug auf die Verarbeitung der personenbezogenen Daten oder sonst im Zusammenhang mit diesen Daten bei der Auftragsverarbeiterin ermittelt.

(4) Ferner ist die Auftragsverarbeiterin verpflichtet, dem Verantwortlichen sämtliche für dessen etwaige Auskunftspflichten gegenüber Betroffenen oder den zuständigen Behörden erforderlichen und ihm/ihr zur Verfügung stehenden Informationen und Auskünfte zu Erhebung, Speicherung, Verarbeitung und Übertragung von personenbezogenen Daten auf erstes Verlangen unverzüglich und vollumfänglich zu erteilen. Die Auftragsverarbeiterin unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten nach Art. 35, 36 DS-GVO (Datenschutz-Folgenabschätzung und vorherige Konsultation) und erteilt alle hierzu erforderlichen Auskünfte.

(5) Die Auftragsverarbeiterin wird den Verantwortlichen in Verfahren vor der Aufsichtsbehörde, in Bußgeld-, Straf- oder Verwaltungsverfahren, in Auseinandersetzungen mit Betroffenen oder Dritten, die im Zusammenhang mit der Auftragsverarbeitung oder den personenbezogenen Daten stehen, insbesondere bei einer Inanspruchnahme wegen etwaiger Ansprüche nach Art. 82 DS-GVO, nach besten Kräften unterstützen.

(6) Die in den Absätzen 1 bis 5 genannten Supportleistungen werden vom Auftragsverarbeiter im Rahmen des Zumutbaren und Angemessenen unentgeltlich erbracht.

(7) Berichtigungen, Löschungen oder Sperrungen von personenbezogenen Daten nimmt die Auftragsverarbeiterin nur auf Anweisung bzw. nach vorheriger Zustimmung des Verantwortlichen vor.

Die Auftragsverarbeiterin ist verpflichtet, ihre Infrastruktur so zu gestalten und alle weiteren Vorkehrungen zu treffen, damit sie den Vorgaben des Verantwortlichen unverzüglich nachkommen kann. Er/Sie unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten und im Rahmen der Weisungen des Verantwortlichen bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO.

(8) Die Auftragsverarbeiterin sichert zu, eine*n fachkundige*n und zuverlässige*n betriebliche*n Datenschutzbeauftragte*n bestellt zu haben, der/dem die erforderliche Zeit zur Erledigung ihrer/seiner Aufgaben nach Art. 38 und 39 DS-GVO gewährt wird. Er/sie teilt dem Verantwortlichen die Kontaktdaten unverzüglich mit. Das gilt auch für eventuelle Wechsel der/des Datenschutzbeauftragten.

§5 Vertraulichkeitsverpflichtung

(1) Die Auftragsverarbeiterin gewährleistet, dass sie die mit der Verarbeitung der Daten des Verantwortlichen befassten Beschäftigten und andere für den/die Auftragsverarbeiterin tätigen Personen untersagt ist, die Daten außerhalb der Weisungen des Verantwortlichen zu verarbeiten. Ferner gewährleistet der/die Auftragsverarbeiterin, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(2) Die Auftragsverarbeiterin sichert zu, dass sie die für den Auftrag eingesetzten Beschäftigten und andere für den/die Auftragsverarbeiterin tätigen Personen mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht hat. Sie überwacht die Einhaltung der datenschutzrechtlichen Vorschriften und der Weisungen.

§6 Technische und Organisatorische Maßnahmen

(1) Die Auftragsverarbeiterin wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, um - ausgehend von der durch den Verantwortlichen festgelegten Schutzstufe der Daten – ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die technischen und organisatorischen Maßnahmen müssen den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen und die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, insb. durch mögliche Verletzungen des Schutzes personenbezogener Daten gemäß Art. 32 Abs. 2 DS-GVO, zu berücksichtigen.

(3) Die von der Auftragsverarbeiterin zu ergreifenden technischen und organisatorischen Maßnahmen können bei Bedarf unter privacy@mpi.nl, Betreff “TOM’s IDLAS” angefragt werden.

(4) Die Auftragsverarbeiterin setzt ein Verfahren gemäß Art. 32 Abs. 1 lit. d) DS-GVO zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ein und informiert den Verantwortlichen über die Ergebnisse der Überprüfung.

(5) Die Auftragsverarbeiterin berät und unterstützt im Rahmen ihrer Möglichkeiten den Verantwortlichen bei der Auswahl und Umsetzung der geeigneten technischen und organisatorischen Maßnahmen, um die Datenschutzgrundsätze der Datenschutz-Grundverordnung (z.B. Datenminimierung) wirksam umzusetzen, die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen (‚Privacy by design'). Gleiches gilt für technische und organisatorische Maßnahmen, die sicherstellen, dass durch die Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist (‚Privacy by default').

(6) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Sämtliche Änderungen sind schriftlich (Textform genügt) zu vereinbaren.

(7) Sensible Daten dürfen ausschließlich über verschlüsselte Verbindungen oder in verschlüsselter Form übertragen werden. Wird für die Entschlüsselung ein Kennwort oder eine andere Form von Schlüsselmaterial benötigt, ist dieses auf einem anderen Wege als der zu verschlüsselnden Verbindung zu übertragen. Mitteilungen der Vertragsparteien per E-Mail bezüglich Datenschutzes, Geheimhaltung und Sicherheit werden nur akzeptiert, wenn das Textstück mit einer digitalen Signatur versehen worden ist. Die Auftragnehmerin trägt bei ihr anfallende Kosten selbst.

(8) Ausgehende E-Mails der Beschäftigten der Auftragsverarbeiterin sind standardmäßig mit einer fortgeschrittenen digitalen Signatur zu signieren. Werden besondere Kategorien von personenbezogenen Daten im Sinne des Art. 9 DS-GVO sowie vertrauliche Daten per E-Mail kommuniziert, hat die sichere Kommunikation per E-Mail mittels End-zu-End-Verschlüsselung zu erfolgen. Der Verantwortliche verwendet hierzu Verschlüsselungtechniken. Die Auftragsverarbeiterin stellt während der gesamten Vertragslaufzeit sicher, dass ihre Beschäftigten entsprechende Mail-Clients mit Signatur und Verschlüsselungsfunktion sowie über gültige Zertifikate verfügen, die den Mindestanforderungen der "Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signatur-verordnung (Übersicht über geeignete Algorithmen)" entsprechen und die von einer gängigen Zertifizierungsstelle ausgestellt sind. Benötigt der/die Empfänger*in für die Entschlüsselung ein Kennwort oder eine andere Form von Schlüsselmaterial, ist dieses auf einem anderen Wege als der zu verschlüsselnden Verbindung zu übertragen.

Die Auftragsverarbeiterin trägt bei ihm anfallende Kosten der digitalen Signatur und Verschlüsselung selbst.

§7 Nachweise und Kontrollrechte des Verantwortlichen

(1) Die Auftragsverarbeiterin weist dem Verantwortlichen die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Der Verantwortliche hat das Recht, mit der Auftragsverarbeiterin Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer, durchführen zu lassen. Bei der Auswahl des Prüfers ist auf die Interessen der Auftragsverarbeiterin angemessen Rücksicht zu nehmen. Der Verantwortliche hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieses Vertrags durch die Auftragsverarbeiterin in deren Geschäftsbetrieb zu überzeugen. Bei der Durchführung der Stichprobenkontrollen im Geschäftsbetrieb der Auftragsverarbeiterin ist auf die Belange und die störungsfreien Betriebsabläufe der Auftragsverarbeiterin angemessen Rücksicht zu nehmen.

(3) Die Auftragsverarbeiterin stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten der Auftragsverarbeiterin nach Art. 28 DS-GVO überzeugen kann. Die Auftragsverarbeiterin verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(4) Die Auftragsverarbeiterin kann auch folgende Nachweise vorlegen:

(4.1) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

(4.2) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

(4.3) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).

Die Rechte des Auftraggebers nach Abs. 2 und 3, Überprüfungen durchzuführen und Auskunft zu verlangen, bleiben unberührt.

(5) Abweichend von § 10 (Vergütung) tragen die Parteien die jeweils auf ihrer Seiten anfallenden Kosten für eine Überprüfung vor Ort nach Absatz 2 selbst.

§8 Unterauftragsverhältnisse

(Bewusst frei gelassen)

§9 Rückgabe, Löschung und Beendigung

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung des Auftrages – hat die Auftragsverarbeiterin die Daten des Verantwortlichen sowie die weiteren Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, sämtliche in seinen Besitz gelangten Unterlagen sowie erstellte Verarbeitungs- und Nutzungsergebnisse dem Auftraggeber nach dessen schriftlicher Anweisung auszuhändigen oder datenschutzkonform zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung oder der Vernichtung ist auf Anforderung vorzulegen.

(2) Unberührt bleiben Sicherungskopien zur Erfüllung von Haftungs- und Gewährleistungsansprüchen. Die Auftragsverarbeiterin wird diese Gegenstände bis zu deren vollständiger Übergabe an den Verantwortlichen für diesen verwahren und ihm auf erstes Anfordern herausgeben. Die Auftragsverarbeiterin sichert diese Gegenstände insbesondere durch ordnungsgemäße Verwahrung und Archivierung gegen Beschädigung und Verlust. Sicherungskopien sind durch geeignete Maßnahmen zu sperren, so dass eine Nutzung den/die Auftragsverarbeiter*in ausgeschlossen ist. Die Auftragsverarbeiterin erteilt dem Verantwortlichen jederzeit Auskunft über solche Sicherungskopien.

(3) Nicht mehr benötigte Unterlagen und Dateien dürfen erst nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen datenschutzgerecht unter Erbringung eines Nachweises vernichtet werden.

(4) Dokumentationen, die dem Nachweis der Auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Verantwortlichen entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

§10 Haftung

Abweichend von der Regelung des Hauptvertrages und soweit in dieser Vereinbarung nicht anders geregelt, vereinbaren die Vertragspartner Folgendes in Bezug auf die Verarbeitung von personenbezogenen Daten:

(1) Die Parteien haften gegenüber Dritten nach Maßgabe des Art. 82 DS-GVO.

(2) Der Innenausgleich zwischen dem Verantwortlichen und der Auftragnehmerin richtet sich nach Art. 82 Abs. 5 DS-GVO.

(3) Für eventuelle Geldbußen i.S.v. Art. 83 DSGVO und/oder andere Sanktionen i.S.v. Art 84 DSGVO des Verantwortlichen gilt diese Regelung entsprechend.

§11 Außerordentliche Kündigung

(1) Verstößt die Auftragnehmerin gegen ihre in diesem Vertrag genannten Pflichten, stellt dies zudem einen außerordentlichen Kündigungsgrund dar.

§12 Schlussbestimmungen

(1) Sollten Daten des Verantwortlichen bei der Auftragsverarbeiterin durch Maßnahmen Dritter (z.B. Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der die Auftragsverarbeiterin den Verantwortlichen unverzüglich zu verständigen. Die Auftragsverarbeiterin hat außerdem den Dritten darauf hinzuweisen, dass es sich um Daten des Verantwortlichen handelt und die Auftragsverarbeiterin die Daten nur im Auftrag verarbeitet.

(2) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(3) Bei etwaigen Widersprüchen zu anderen vertraglichen Regelungen gehen hinsichtlich des Datenschutzes die Regelungen dieses Vertrags vor.

(4) Änderungen und Ergänzungen dieses Vertrags und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(5) Sollte eine Bestimmung dieses Vertrages unwirksam sein, bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien sie durch eine neue Bestimmung ersetzen, die dem, was die Parteien gewollt haben, möglichst nahe kommt.

(6) Die Verarbeitung von personenbezogenen Daten sowie dieser Vertrag unterliegen deutschem Recht.

Ort, Datum	Ort, Datum
Für den Verantwortlichen handelnd für das MPI für […]	Für die Auftragsverarbeiterin
Geschäftsführende*r Direktor*in (oder vertretungsberechtigte Funktion) Titel und Name	