

DATA PROCESSING AGREEMENT IN CON- FORMITY WITH ART. 28 GENERAL DATA PROTECTION REGULATION

[Information how to use the template:

- i. Please coordinate your document within the MPI and if applicable with Administrative HQ, before forwarding it to the Processor.
- ii. Please delete or integrate any highlighted completion aids (yellow), notes (turquoise) and alternative regulation (grey) after editing and before forwarding the template to the Processor.

The

Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.
(registered in the Register of Associations in Berlin)

– hereinafter referred to as the “**MPG**” –

represented r by the **Managing Director ...**

acting for the

Max Planck Institute of/for ...
[Address]

– hereinafter referred to as the “**MPI**” –

– MPG and MPI jointly referred to hereinafter as “**Controller**” –

and

.....

[Address]

represented by **NAME**

– hereinafter referred to as “**Processor**” –

– MPG and Processor hereinafter jointly referred to as “**Parties to the Agreement**” –

conclude the following contract (hereinafter: “**Agreement**”):

Contents

§1	Subject of the contract.....	2
§2	Scope, type and purpose of the personal data processing	2
§3	Rights and obligations of the Controller.....	4
§4	Rights and obligations of the Processor	4
§5	Confidentiality obligations	5
§6	Technical and organizational measures	5
§7	Evidence of compliance and Controller's rights of control.....	6
§8	Subcontracting relationships	Fehler! Textmarke nicht definiert.
§9	Surrender, deletion and end of Agreement	7
§10	Fees	7
§11	Liability	8
§12	Contractual penalty	8
§13	Extraordinary termination	8
§14	Closing provisions.....	9

§1 Subject of the contract

- (1) O1:
The Processor performs the processing activities specified in the Contract _____ of <Date DD.MM.YYYY> (hereinafter: Main Contract].
- O2:
The Processor performs the following processing activity:
- O3:
The Processor performs the processing activities specified in the Contract _____ of <Date DD.MM.YYYY> (hereinafter: Main Contract] and the following processing activities:
- (2) The Processor performs the processing activities of the Agreement in accordance with the subject and duration of the Main Contract.

§2 Scope, type and purpose of the personal data processing

- (1) O1:
The Processor processes the following types of personal data:
- _____
- The Processor processes the following categories of personal data:
- _____
- Personal data is processed for the following purposes:
- _____
- O2:
Annex X describes the type and purpose of data processing as well as the categories of data subjects.

(2) According to the Controller's Security Levels Concept, the personal data are classified in the following:

O1:
normal

O2:
high

O3:
very high

(3) The Processor collects, processes or uses the personal data only within the scope of the documented instructions of the Controller. The Processor is bound by the Controller's instructions during the entire term of the Agreement.

(4) O1:
The Processor only processes personal data in countries which are members of the European Union or signatory states to the Agreement on the European Economic Area. The Processor hereby warrants to protect the personal data from access by state authorities outside the European Union or the European Economic Area.

O2:
The Processor only processes and stores personal data in countries that are members of the European Union or signatory states to the Agreement on the European Economic Area or in countries which have an adequate data protection level (so-called White-List countries) according to a decision of the EU Commission pursuant to Art. 45 GDPR. The Processor hereby warrants to protect the personal data from access by state authorities outside the European Union or the European Economic Area or White-List countries.

O3:
Personal data will be processed and stored in the following countries:

- [REDACTED]

An adequate data protection level is ensured through:

- [REDACTED]

The Processor hereby warrants to protect the personal data from access by state authorities outside the European Union or the European Economic Area or White-List countries.

(5) O1:
Any transfer of personal data to a third country requires the prior consent of the Controller and will only be affected if the specific requirements of Art. 44 et seq. GDPR are fulfilled. The specific requirements will the Parties specify in a separate agreement.

O2:
Any further transfer to a third country requires the prior consent of the Controller and will only be affected if the specific requirements of Art. 44 et seq. GDPR are fulfilled. The specific requirements will the Parties specify in a separate agreement.

O3:
The Processor notifies the Controller be notified of planned changes in good time. Any such change requires the prior consent of the Controller and will only be affected if the specific requirements of Art.s 44 et seq. GDPR are fulfilled. These are to be specified in a separate agreement.

- (6) The Processor uses data only for the in this Agreement specified purposes. Except for back-up copies to ensure orderly data processing or to fulfil liability and warranty claims the Processor does not copy or duplicate personal data without Controller's knowledge and written consent.
- (7) The Processor does not give personal data to third parties, including data protection supervisory authorities, without consulting the Controller first.

§3 Rights and obligations of the Controller

- (1) The Controller is the "responsible party" within the meaning of Art. 4 No. 7 GDPR for processing of data. The Controller is responsible for assessing the lawfulness of data processing.
- (2) The Controller is responsible for safeguarding the rights of data subjects. The Processor informs the Controller without undue delay if data subjects assert their rights against the Processor.

(3) O1:

The Controller instructs the Processor to comply with all obligations under the Agreement. The controller is entitled to issue additional instructions to the processor at any time regarding the type, scope and nature of data processing. Instructions are issued in writing or via email with a digital signature.

O2:

The Controller instructs the Processor to comply with all obligations under the Agreement. The controller is entitled to issue additional instructions to the processor at any time regarding the type, scope and nature of data processing. Instructions are issued in writing or via email bearing a digital signature.

Authorised to give instructions on part of the Controller is:

- [REDACTED]

- (4) The Controller informs the Processor without undue delay if the Controller discovers any errors or irregularities regarding data protection provisions.

§4 Rights and obligations of the Processor

- (1) The Processor regularly monitors data processing activities and internal processes and informs the Controller without undue delay of any potential data breach, cases of serious operational disruptions or other irregularities regarding the Controller's personal data. In case of a potential data breach, cases of serious operational disruptions or other irregularities regarding the Controller's personal data the Processor takes all necessary measures to safeguard Controller's personal data and to mitigate any possible effects for the personal data subjects and consults the Controller without undue delay. The Processor provides the Controller with all requested information without undue delay, in particular with the information required for notifications according to Art. 33, 34 GDPR, and supports the Controller in fulfilling their obligations in accordance with Art. 33, 34 GDPR. The Processor allows without undue delay the Controller or third parties acting for the Controller, to conduct their own investigations into the personal data processing.
- (2) The Processor informs the Controller without undue delay in the event they believe that an instruction is in violation of the GDPR or the personal data protection provisions of the EU or its member states.
- (3) The Processor notifies the Controller prior to an announced inspection by a data protection supervisory authority, if the Controller's data or the services the Processor performs for the Controller are affected by the inspection. The Processor also notifies the Controller if an inspection by the supervisory authority effects how the Processor's obligations under the Agreement is fulfilled by the Processor. The Processor also notifies the Controller whenever an authority investigates the Processor as part of criminal or fining proceedings that effects Controller's personal data.
- (4) The Processor provides the Controller with all information about collecting, storing, processing and transfer of personal data upon first request so the Controller can fulfil its legal information obligations to data subjects or the personal data protection supervisory authorities.
- (5) The Processor supports the Controller to the best of their ability in proceedings before the supervisory authority, in fine proceedings, criminal or administrative proceedings, in disputes with data subjects or third parties, in particular in the event any claims under Art. 82 GDPR.

- (6) The Processor will only correct, delete or block personal data if instructed so by or with the prior consent of the Controller.
- (7) The Processor sets up its infrastructure and to take all further precautions so that the Processor always complies with the Controller's requirements. The Controller supports the Controller to the best of their ability and within the scope of the Controller's instructions to fulfil requests and claims of data subjects under Chapter III GDPR.

(8) O1:

The Processor appoints a competent and reliable Data Protection Officer who is able to fulfil the tasks according to Art. 38 and 39 GDPR. The Processor gives the Controller the Data Protection Officer's contact details and if so of a new Data Protection Officer.

O2:

The Processor is not obliged by law to appoint a Data Protection Officer.

- (9) The Processor's Data Protection Officer is:

§5 Confidentiality obligations

- (1) The Processor prohibits its employees as well as any other persons or party working for the Processor to process the personal data beyond the Controller's given instructions. Furthermore, the Processor ensures that the persons processing the personal data agreed to confidentiality or are obliged to confidentiality by law. The obligation of confidentiality continues for a period of 3 years after the Agreement has ended.
- (2) The Processor familiarizes its with employees as well as any other person or party working for the Processor with all to applicable data protection provisions. The Processor monitors its compliance with data protection regulations and with the Controller's instructions.

§6 Technical and organizational measures

- (1) The Processor designs its internal organisation to meet the data protection requirements. The Processor implements technical and organizational measures based on the Security Level of the personal data as determined by the Controller to adequately protect the Controller's personal data.
- (2) These technical and organizational measures meet the requirements of the General Data Protection Regulation (Art. 32 GDPR) and long term ensure confidentiality, integrity, availability and resilience of the systems and services in connection with the personal data processing. The Processor thereby takes into account the state of art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, in particular through possible violations of the protection of personal data pursuant to Art. 32(2) GDPR.
- (3) The technical and organizational measures that the Processor implements are defined in **Annex X**.
- (4) The Processor regularly reviews pursuant to Art. 32(1) (d) GDPR the effectiveness of the technical and organizational measures to ensure the safety of the processing and informs the Controller of the results of the review .
- (5) Within the scope of their capabilities, the Processor advises and supports the Controller in choosing and implementing appropriate technical and organisational measures to meet the Controller's data protection obligations according to the General Data Protection Regulation (e.g. data minimization), to incorporate the necessary according to the General Data Protection Regulation and to protect the rights of the personal data subjects according to the General Data Protection Regulation (privacy by design). The Processor also advises and supports the Controller in taking technical and organisational measures to ensure that, by default, only personal data whose processing is necessary for the specific purpose of the processing are processed (privacy by default)..

- (6) To the extent necessary during the Agreement the Parties adjust the technical and organisational measures to the further technical and organisational development. **all changes must be agreed by the parties in writing.**
- (7) Sensitive data are transmitted via encrypted connections or in encrypted form only. If the recipient requires a password or other key material for decryption, the password or other key material for decryption is transmitted through a different. Any communication of the Parties via email regarding data protection, confidentiality and security are only accepted if the text of the email has a digital signature. The Processor bears its own costs for the digital signature and encryption.
- (8) The Processor's employees by default sign outgoing emails with an advanced digital signature.
If sensitive personal data within the meaning of Art. 9 GDPR as well as confidential data are transmitted via email, the secure email communication the Parties use end-to-end encryption. For this purpose, the Controller uses encryption. The Processor warrants throughout the entire term of the contract that their employees have appropriate email clients with signature and encryption functionality as well as valid certificates that meet the minimum requirements of the "Announcement concerning electronic signatures pursuant to the Digital Signature Act and the Digital Signature Ordinance (overview of suitable algorithms)" and that have been issued by an established certification authority. If the recipient requires a password or any other form of keying material for decryption, this must be transmitted by a means other than the connection to be encrypted.
The Processor bears its own costs for the digital signature and encryption .

§7 Evidence of compliance and Controller's rights of control

- (1) The Processor proves the Controller in writing its compliance with the obligations stipulated in this Agreement.
- (2) The Controller has the right to audit the Processors either itself or by an appointed representative. When selecting its appointed representative, the Controller has to give consider legitimate interests of the Processor. The Controller has also the right audit the Processor on the Processor's business sites. The Controller usually notifies the Processor about an on-site audit in advance. . The Controller tries to avoid disruptions with the Processor's business operations during on-site audit.
- (3) The Processor allows that the Controller is able to verify the Processor's compliance with its obligations pursuant to Article 28 GDPR. The Processor provides upon request the Controller with all necessary information and, in particular, prove its compliance with the technical and organizational measures.
- (4) The Processor provides at least one of the following proof:
- (4.1) Certification by an approved certification procedure pursuant to Art. 42 GDPR;
 - (4.2) Current certificates, reports or extracts from reports by independent bodies (e.g. auditors, data protection officer, IT security department, data protection auditors, quality auditors);
 - (4.3) appropriate certification by IT security or data protection audit (e.g. in accordance with BSI Grundschutz).
- The Controller's rights pursuant to paras. 2 and 3 to audit on the Processor's business sites and to information remain unaffected hereby.

(5) O1:

Notwithstanding § 10 (Fees), the Parties each bear their own costs for an on-site audits pursuant to para. 2.

O2:

Notwithstanding § 10 Fees, the Parties each bear their own costs for an on-site inspection pursuant to para. 2, unless a breach of statutory provisions regarding protection of personal data or a breach of the provisions of this Agreement by the Processor(s) was the reason for the Controller's on-site audit pursuant to para. 2.

§8 Subcontracting Processors

- (1) The Controller approves to the subcontracting processors (hereinafter referred as "Sub-processors") in **Annex X**.

- (2) The Processor informs the Controller of any intended change in the sub-processors. The Controller is entitled to object to such changes.
- (3) The Processor ensures in a contract with the Sub-processor that the Sub-processor has the same obligations directly towards the Controller as the Processor has towards the Controller under this Agreement. The Processor verifies before the start of data processing and at regular intervals thereafter, the Sub-processors compliance with its contractual obligations and obligations by law, in particular compliance with the technical and organizational measures agreed in the Agreement. The Processor documents results in writing. The Processor is legally responsible if its Sub-processor(s) fail(s) to meet their data protection obligations.
- (4) The Processor ensures in a contract that the Controller has the same control rights directly towards the sub-processors as the Controller towards the Processor, irrespective of the Processor's own responsibility for the Sub-processor. - The Processor gives the Controller upon request the contract with the Sub-processor, and any information about the Subprocessors' implementation of the personal data protection obligations.
- (5) The Processors does not transfer Controller's personal data to the Sub-processors until the Sub-processors meet all requirements for proper data processing.
- (6) The sub-processors do not use further sub-processors. The Processor prohibits in its contract with the Sub-processors the use of further Sub-processors.
- (7) Ancillary service providers ; for example, telecommunications services, postal/transport services, maintenance and user services, the disposal of data carriers and measures taken to ensure the confidentiality, availability, integrity and resilience of the software and IT systems are not Sub-processors. The Processor still concludes appropriate and legally compliant contract with these ancillary service providers and takes control measures to ensure protection and security of the Controller's personal data.

§9 Surrender, deletion and end of Agreement

- (1) Upon completion of the Processor's services or earlier upon the Controller's request, but at the latest upon termination of the Main Contract, the Processor surrenders any of the Controller's personal data, all and any documents which are in the Processor's possession as well as the results obtained from the personal data processing and use of the personal data to the Controller in accordance with the latter's written instructions or destroys them in compliance with personal data protection law. The same applies for test materials and discarded materials. The Processor has to proof deletion or destruction of the personal data upon request.
- (2) However, backup copies which have been made in order to fulfil liability and warranty claims remain unaffected. The Processor keeps these items safe until their complete handover to the Controller upon the Controller's request.. The Processor secure these items against damage or loss, in particular by storing and archiving them properly. The Processor locks Backup copies so that an independent use by the Processor is not possible. The Processor informs the Controller that the Processor made back-up copies .
- (3) Only with the Controller's prior written consent the Processor is allowed to data protection law compliant destroy documents and files that are no longer needed and proofs the destruction of the documents and files to the Controllers.
- (4) The Processor keeps documentation as proof of personal data processing as well as of its compliance after the end of the term of the Agreement in accordance with the respective retention periods given by the Controller. The Processor is allowed to hand the documentation over to the controller for their discharge when the Agreement terminates.

§10 Fees

(1) O1:

The Processor performs the services stipulated in this Agreement free of charge.

O2:

The Processor performs the support services referred to in XY free of additional charge, insofar as they are reasonable and appropriate for the Processor.

(2) O1:

To the extent that the support services referred to in para. 1 are not reasonable for the Processor, the Processor is allowed to charge additional compensation. The terms of remuneration and payment of the Main Contract apply.

O2:

To the extent that the support services referred to in para. 1 are not reasonable for the Processor, the Processor is allowed to charge additional compensation exclusive of statutory VAT at the rate applicable at the time of the service being provided:

Service/position	Price / unit	Agreed cap
Service/position Y	EUR X/unit	EUR X
TOTAL:		EUR XXX

The Processor proves to Controller in writing of the time spent performing the service, including a detailed description of the services based on the type of service, the time, qualification and person. The Controller has sign the proof before the Processor is allowed to invoice its services.

§11 Liability

Notwithstanding the provisions of the Main Contract and unless otherwise stipulated in this Agreement, the Parties agree:

- (1) The Parties are liable to third parties in accordance with Art. 82 GDPR.
- (2) The compensation between Controller and Processor is governed by Article 82(5) GDPR.
- (3) § 11 (2) also applies accordingly to any fines if the Controller is fined within the meaning of Article 83 GDPR and/or other sanctions within the meaning of Article 84 GDPR.

§12 Contractual penalty

- (1) The Parties agree that pecuniary damages alone are not sufficient to compensate for a breach of this Agreement.
- (2) The Controller therefore has the right to a contractual penalty of up to EUR [XY.-] from the Processor for each individual culpable breach of §§ 2 through 9 by the Processor. The legal principles of continuation or continuation-in-part (Grundsätze des Fortsetzungszusammenhangs) are excluded. In total, however, the sum of the contractual penalties to be paid on the basis of this provision may not exceed 10% of the contract value.
- (3) The payment of the contractual penalty shall not exclude the assertion of a claim for injunctive relief or further damages upon corresponding proof. The contractual penalty shall be offset against any possible damages.

§13 Extraordinary termination

- (1) If the Processor breaches its obligations stipulated in this Agreement, the Controller has the right to terminate the Agreement early.
- (2) In this case no additional termination of the Main Contract is required.

§14 Closing provisions

- (1) With the exception of § 13 the term of this Agreement corresponds to the term of the Main Contract. § 13 remains unaffected by this. If the Main Contract ends, this Agreement automatically also ends. A separate termination of the Agreement is not required.
- (2) If personal data of the Controller is subject to third-party measures (e.g. attachment or seizure), to insolvency proceedings or composition proceedings or to other measures, the Processor informs the Controller about these measures and proceedings without undue delay. The Processor also notifies the third party that the personal data subject to these measures and proceedings belongs to the Controller and that the Processor is only processing the personal data on behalf of the Controller.
- (3) The defence of the right of retention pursuant to § 273 of the German Civil Code (BGB) (Zurückbehaltungsrecht) is excluded with regarding the Controller's personal data and the associated data media.
- (4) In the event of any conflict with the provisions of the Main Contract or other Contracts between the Controller and the Processor, the provisions of this Agreement take precedence regarding the protection of personal data.
- (5) Amendments and supplements to this contract and any and all of its components - including any warranties of the Processor - must be in a written agreement, and the express indication that it is an amendment or supplement to this Agreement. This also applies to the waiver of this formal requirement.
- (6) The processing of personal data and this Agreement are subject to German law.
- (7) The following Annexes are attached to this Agreement:
 - Annex 1 Description of the type and purpose of the personal data processing as well as the groups of personal data subjects
 - Annex 2 Technical and organizational measures (TOM)
 - Annex 3 Authorized sub-processors

Place, date	Place, date
For the Controller acting on behalf of the MPI of/for [...]	For the Processor
Managing Director (or authorized representative) title and name	

Please note that this version has been produced by the translation agency commissioned by the MPG.
If you have any suggestions for making this English document more readily comprehensible, we would be very pleased to hear from you at ohb@gv.mpg.de.