Terms of Service

1 Subject Matter of the Agreement

1.1 Subject to the terms of this Platform-as-a-Service Agreement including the order form and its Annexes ("**Agreement**"), mogenius provides Customer with the services as set out in this Agreement including the relevant order form and as specified in the service specification in ("**Service Specification**"), together, the "**Services**".

1.2 Subject to the terms of this Agreement and as consideration for the provision of the Services, Customer pays to mogenius the Fees set out in this Agreement in accordance with the applicable parts of this Agreement (as specified the order form).

2 Conclusion of the Agreement; B2B Services

2.1 This Agreement can be concluded in writing (including electronic form).

2.2 The signatory confirms to be duly authorized to enter into this Agreement on behalf of Customer.

The Agreement is concluded with the completion of the order form and the execution of the Agreement by both Parties, either in writing or through DocuSign or a similar electronic signature process. Customer shall receive a copy of the Agreement document in paper form or as an electronic copy.

2.3 Upon signature of the Agreement by both Parties, mogenius shall set up Customer's cloud workspace and send Customer instructions how to create a user account allowing Customer to use the Services. Alternatively, Customer can name an existing cloud workspace which mogenius shall upgrade according to the terms of this Agreement.

2.4 This Agreement and the Services are directed only at entrepreneurs (*Unternehmer*). mogenius reserves the right to request suitable information and to demand proof that Customer is not a consumer.

2.5 General terms and conditions of Customer shall only become part of the Agreement if mogenius expressly agrees to them in writing.

3 Services

3.1 General provisions

3.1.1 mogenius sets up, provides and maintains the Services throughout the Term in the manner, form, to the extent and on the basis of the service levels as set out in the Service Specification.

3.1.2 mogenius shall be responsible for operation and maintenance of the Services. If mogenius provides mogenius Cloud Hosting Services, the place of service delivery is the router exit of the data centre commissioned by mogenius.

3.1.3 Customer is responsible for providing all equipment required to access the Services, including without limitation all software, third-party services to upload data and any hardware required on Customer's side.

3.1.4 Notwithstanding any restrictions under applicable data protection laws and unless expressly agreed otherwise, mogenius shall have the right to subcontract its obligations under this Agreement to third-party agents and assistants (*Erfüllungsgehilfen*). mogenius shall be liable for any acts and/or omissions of any such third-party agents and assistants in accordance with applicable law.

3.1.5 If mogenius provides mogenius Cloud Hosting Services, mogenius performs backups of all data stored on systems provided to Customer under this Agreement as set out in the Service Specification. In the event of data loss, mogenius shall rollback the last available backups to its systems upon Customer's request or in its discretion. Customer is not entitled to directly access backups created by mogenius and mogenius is not obligated to individually check the correctness and completeness of the backups performed for Customer. Customer agrees and acknowledges that the general system backups created by mogenius alone are not sufficient for a state-of-the-art backup strategy. Customer is obligated to perform independent backups of any data stored on mogenius' systems according to the sensitivity of the data and the level of protection required by Customer, to the extent that Customer has access to the data.

3.1.6 If the Services include access to application programming interfaces ("**API**") provided by mogenius, Customer is solely responsible for the implementation of the API as well as the installation, operation and maintenance of its application making use of the API ("**Application**"), including compliance of its application with all applicable laws, regulations and other third-party requirements. To the extent reasonable and technically possible, Customer must take precautions during the implementation of the Application using the API to ensure that Customer's Application will continue to work properly even if the API is not available, whether caused by mogenius' or Customer's fault.

3.1.7 mogenius shall provide Customer with a reasonable documentation of the Services in electronic form and in English language.

3.2 **Bring Your Own Cloud**

3.2.1 If Customer choses to host the Services on Customer's own cloud environment ("**Third-Party Cloud**"), mogenius shall set up the Services in Customer's Third-Party Cloud and shall maintain the Services during the Term and as long as Customer grants mogenius the required access to the Third-Party Cloud provided that and as long as the Third-Party Cloud complies with the technical requirements agreed between the Parties at the time of the setup of the Services on the Third-Party Cloud ("**Bring Your Own Cloud Services**"). Customer is solely responsible to maintain mogenius' access to the Third-Party Cloud and to ensure that the technical requirements to use the Services on the Third-Party Cloud will be met at all times.

3.2.2 Customer shall provide all information and access to the Third-Party Cloud to mogenius reasonably necessary and requested by mogenius to set up the Services on Customers cloud environment.

3.2.3 Any use of Third-Party Cloud services is exclusively subject to the terms and conditions agreed between Customer and the provider of the respective Third-Party Cloud ("**Third-Party Cloud**

Provider"). mogenius is not responsible for the proper provision or operation of any Third-Party Cloud, including without limitation any interruptions of Third-Party Cloud services.

3.3 Third-Party Services

3.3.1 mogenius may provide features which allow Customer to interact with the mogenius Services through third-party services used by Customer ("**Third-Party Services**") or to interact with Third-Party Services through the mogenius Services ("**Third-Party Integrations**"). In such case, mogenius shall only provide technical means for the mogenius Services to interact with such Third-Party Services to the extent and within the scope agreed between the Parties.

3.3.2 Any use of Third-Party Services is exclusively subject to the terms and conditions agreed between Customer and the provider of the respective Third-Party Service ("**Third-Party Services Provider**"). mogenius is not responsible for the proper provision or operation of any Third-Party Service.

4 Changes to the Services

mogenius may introduce changes to the Services in the following cases:

4.1 Additional services

mogenius may add additional features to the Services at any time. Features added by mogenius after the conclusion of this Agreement are, unless expressly agreed otherwise, considered additional services provided free of charge. mogenius is entitled to deprecate such additional services reasonably considering the interests of both Parties. mogenius may offer additional services and further developments only against payment of an additional fee.

4.2 API

mogenius may introduce new separate versions of its API extending, changing or limiting the scope of features at any time. If mogenius provides a new version of the API, Customer shall implement the new version of the API into its Application within a reasonable period of time from the announcement of the new API version, considering the extent of the changes, usual development time in the industry and the justified interests of Customer, including the individual capacities of Customer. mogenius may deprecate former versions of the API under the conditions set out in Section 4.6.

4.3 Bring Your Own Cloud

In the event that a Third-Party Cloud Provider significantly changes, limits or deprecates Third-Party Cloud services required by mogenius to provide the Services, mogenius may change, limit or deprecate the Services for the respective Third-Party Cloud accordingly, reasonably considering the legitimate interests of both Parties. mogenius shall notify Customer of such changes in writing (e-mail sufficient), if reasonably possible considering whether and when mogenius has been notified of changes made by Third-Party Cloud Providers, before the changes come into effect.

4.4 Third-Party Integrations

Third-Party Integrations depend on the support and interfaces provided by the respective Third-Party Services Provider. In the event that a Third-Party Services Provider significantly changes, limits or deprecates the support or interfaces required by mogenius to provide the Third-Party Integrations, mogenius may change, limit or deprecate Third-Party Integrations accordingly, reasonably considering the legitimate interests of both Parties. mogenius shall notify Customer of such changes in writing (e-mail sufficient), if reasonably possible considering whether and when mogenius has been notified of changes made by Third-Party Services Providers, before the changes come into effect.

4.5 **Reasonable or insignificant changes**

mogenius is entitled to change, limit or deprecate features or parts of the Services or amend technical requirements of the use of Services on a Third-Party Cloud or Third-Party Integration to an extent reasonable for the Customer. Such changes shall be deemed reasonable in particular if they only concern insignificant components of the Services (such as mere design changes that do not or only slightly affect the functionality of the Services) or become necessary for an important reason, including without limitation if

a) disruptions in the provision of Services by mogenius' subcontractors,

b) the change is required for security reasons,

c) the change is required due to changes in applicable law, or

d) there are similar important reasons, and the change is reasonable for Customer after duly taking his interests into account.

Subject to Section 4.6, any change shall essentially maintain the scope of Services as set out in this Agreement and shall not limit mogenius’ main performance obligations.

If a change does not exclusively concern time-critical security updates, additional services or insignificant components of the Services, mogenius shall notify Customer of the change in writing (e-mail sufficient) at least 2 weeks before the change comes into effect.

4.6 **Other changes**

mogenius may also make changes to the Services or technical requirements of the use of Services on a Third-Party Cloud or Third-Party Integration in cases other than those specified in clauses 4.1, 4.2 and 4.3 and under consideration of the interests of both Parties. In this case, mogenius shall notify the Customer of the planned changes 2 months prior to the introduction of the changes. During this time the Customer has the right to object to the proposed changes. If the Customer does not object during this period, the changes shall be deemed to have been approved by Customer. mogenius shall inform the Customer of this legal consequence of his silence in the change notification. If the Customer objects to the changes in due time, mogenius has the right, at its discretion, either to continue to provide the affected Services without the planned changes or to terminate this Agreement with a notice period of 1 month upon receipt of Customer's objection.

5 Availability

5.1 Except for Bring Your Own Cloud Services and Third-Party Services, mogenius shall provide an annual average uptime as set out in the Service Specification. The availability calculation excludes any downtime for planned maintenance work as well as service interruptions which are beyond mogenius' control, including without limitation force majeure.

5.2 Subject to the exceptions in Section 5.1, availability shall be calculated as the number of hours the Services are functional, divided by the total number of hours within the respective calendar year.

5.3 mogenius shall notify Customer in due time in advance of any unavoidable downtime due to planned maintenance work.

6 Copyright and Intellectual Property

6.1 mogenius grants Customer a non-exclusive, non-transferable, worldwide right to use the Services including its documentation for its intended purpose for the term and within the scope of this Agreement. Customer may grant sublicenses to its affiliated companies in terms of Sec. 15 German Stock Act (AktG) ("**Affiliates**"), provided that Customer remains solely and fully responsible for any use of the Services by its Affiliates, has all necessary rights, title, permission and contractual agreements required for fulfilling Customer's obligations under this Agreement and authorisation and ensures that its Affiliates will comply with any applicable law and the terms of this Agreement in its applicable version when using the Services.

6.2 All rights regarding data, content, code or other information ("**Content**") uploaded and/or processed by Customer when using the Services remain with Customer. However, Customer grants mogenius the non-exclusive, sub-licensable, worldwide right to use the Content limited to the extent and for the sole purpose of providing the Services to Customer in accordance with this Agreement and the applicable documentation.

7 Data Protection

To the extent that Customer processes personal data using the Services, the Parties enter into the data processing agreement attached hereto as **Annex 1**.

8 Customer's obligations

8.1 Customer may use the Services solely for the intended or agreed purposes. In particular, Customer may not, and will not allow third parties to use the Services, unless expressly agreed otherwise with mogenius,

a) for any activities infringing applicable laws or regulations, including without limitation distribution of malware, phishing attempts, spamming or other unsolicited advertising;

b) for uploading, storing or distributing any Content which infringes third party rights;

c) to rent, lease or otherwise provide the Services to a third party (excluding Affiliates subject to Section 6.1);

d) to perform benchmark or other capacity testing of the Services or its underlying infrastructure;

e) in connection with or for the purpose of operating critical infrastructure such as electrical power stations, military or defence equipment, medical appliances or other equipment whose failure or impairment would result in unforeseeable economical or physical damages, including but not limited to critical infrastructure in terms of the European Directive 2008/114/EC.

8.2 Customer is only permitted to use the Services in compliance with applicable laws. This also includes export control laws and regulations. In particular, Customer is obligated to observe all legal requirements for the collection, processing and use of data which is transmitted to and processed by the Services for Customer under this Agreement.

8.3 Customer designates a contact person authorized to receive and issue legally binding declarations in connection with this Agreement. Customer shall inform mogenius without undue delay about changes related to this contact person or their contact details.

8.4 Customer is obligated to keep any access credentials provided to access the Services secure and undertakes not to disclose them to any unauthorised third parties unless required for the contractually intended and permitted use of the Services. Customer shall inform mogenius without delay if there is a suspicion that the access credentials may have become known to unauthorized persons.

8.5 Customer is obligated to adhere to any security precautions, functional and other limitations of the Services. In particular, Customer must not bypass, remove, defeat, avoid, deactivate or otherwise circumvent protection or authentication mechanisms or misuse the Services for purposes other than those intended or expressly documented.

8.6 Customer warrants that the Content uploaded and/or processed by Customer when using the Services does not infringe any third-party rights (e.g. intellectual property rights) or any applicable laws and regulations (e.g. data protection legislation), including applications used or intended for spamming, attacks if mogenius' or third-party systems, phishing, crypto mining or malware of any kind ("**Prohibited Content**"). mogenius is entitled to block or delete Prohibited Content after weighing the interests of both Parties, as well as where mogenius is required to do so under applicable law, because of a third-party complaint or a court or administrative order.

8.7 In the event that Customer uses Third-Party Services, Third-Party Cloud services or other third-party applications to access the Services, Customer shall comply with the acceptable policies and terms of services set out by their respective vendor if applicable.

8.8 Customer shall indemnify mogenius from and against any and all third-party claims including necessary industry-standard expenses for legal defence not limited to the statutory fees, asserted against mogenius due to a culpable violation of this Agreement by Customer. If third parties should assert such claims against mogenius, mogenius shall inform Customer about the asserted claims without undue delay and, in mogenius' discretion, leave the defence at the discretion of Customer or undertake it in cooperation with Customer. mogenius shall not settle or recognise claims of third parties without Customer's consent which shall not be unreasonably withheld or delayed. mogenius shall be entitled to request a reasonable advance for the incurred legal defence expenses to be anticipated. The indemnification shall accordingly apply to fines or other regulatory or judicial orders and claims.

9 Restriction of access to the Services

9.1 mogenius is entitled to restrict or block the access of Customer or its users to the Services if

a) there are indications that Customer's access credentials have been or are being misused or the access credentials have been or are being provided to an unauthorized third party or access credentials are being used by more than one natural person;

b) there are indications that unauthorized third parties have otherwise gained access to the Services provided to Customer;

c) the restriction of access is necessary for technical reasons;

d) mogenius is obligated to restrict or block the access or data due to applicable laws or due to judicial or official obligations;

e) mogenius detects Prohibited Content related to Customer;

f) Customer is more than two weeks in delay with the payment of the agreed upon Fee in the sense of Section 11 of the Agreement;

g) Customer has deposited false or invalid contact data and communication between mogenius and Customer is no longer possible;

h) Customer has deposited false bank account data and regular fulfillment of Customer's obligations is not ensured.

9.2 mogenius shall announce the restriction or blocking of Customer's access to the Services to Customer in writing (e-mail sufficient) at least one working day before the restriction or blocking comes into effect, as far as the announcement is reasonable under consideration of the mutual interests and is compatible with the purpose of the restriction or blocking. mogenius shall reinstate Customer's access to the Services where the reason for restriction no longer applies.

10 Term and Termination

10.1 This Agreement shall commence on the Effective Date (as set out in the order form) and remain in force for the Term (as set out in the order form), unless terminated in accordance with this Section.

10.2 Each Party may terminate this Agreement with or without cause with the Notice Period set out in the order form. Termination notices by Customer shall be submitted to mogenius in writing (e-mail sufficient).

10.3 Any mandatory right of the Parties to terminate this Agreement in accordance with applicable law shall remain unaffected. mogenius shall be entitled to terminate this Agreement for good cause in particular where:

a) Customer repeatedly and despite preceding warnings by mogenius, uses the Services to process Prohibited Content;

b) Customer culpably infringes its confidentiality obligations under Section 12 of this Agreement;

c) Customer is more than four weeks in delay with the payment of any agreed and due Fees, and mogenius has announced the termination to Customer in text or written form with a notice period of two weeks to the effective date of termination;

11 Fees

11.1 As consideration for the provision of the Services, Customer pays to mogenius the Fees set out in the order form, consisting of the agreed Base Fees and usage based fees in the event of upgrades ordered by Customer.

11.2 Unless agreed otherwise in the order form, the Fees shall be excluding VAT.

11.3 Unless agreed otherwise in the order form, mogenius shall invoice Customer electronically in the form of PDF-files, stating Customer's full legal name, its post address, date, its VAT ID, unique invoice number, amount of VAT and applicable VAT rate. Fees invoiced in such manner shall be due and paid within the Payment Terms and to the Bank Account or by the payment method agreed between the Parties, each as set out in the order form.

11.4 mogenius may charge Customer the actual costs resulting from an unjustified chargeback, refusal to pay or opening of a dispute by Customer. Should problems arise that prevent the collection/debiting of the invoice amount, mogenius reserves the right to subsequently only offer certain payment methods for the settlement of the following invoices.

12 Confidentiality and Secrecy

12.1 The Parties undertake to treat information or documents pertaining to business, technical, organizational, financial, operational, regulatory or sales-related issues, information and know-how concerning technologies, designs, specifications, products, services, work processes, business relationships including business and cooperation partners, business strategies, or other information pertaining to the disclosing Party's business, whether in oral, written, graphic or other form, (i) which is marked or designated as confidential, or (ii) in which the disclosing Party has an identifiable interest in maintaining the confidentiality of the information involved ("**Confidential Information**") as strictly confidential, to use them exclusively for the purposes of this Agreement and not to make them accessible to third parties. The receiving Party shall take appropriate technical and organizational measures to prevent unauthorized access / disclosure of confidential information. Third parties within the meaning of this Agreement shall also include companies affiliated with the respective receiving Party in which the receiving Party does not hold a majority of capital and voting rights. The employees of the receiving Party as well as other third parties engaged by it (including subcontractors and freelancers) shall be obligated accordingly.

12.2 On the part of mogenius, confidential information shall be deemed to include, in particular, the software of the Services as well as all technologies of mogenius, information provided by mogenius via the Services or in the context of support requests or cooperation for the purpose of troubleshooting, as well as this Agreement including the Annexes and the agreed terms and conditions.

12.3 The receiving Party is entitled to disclose the Confidential Information made available to it to third parties, if and to the extent that this is indispensable for the performance of this Agreement or the exercise of contractual rights or if this is mandatory for legal or regulatory reasons. In the event of requests by third parties, judicial or administrative authorities regarding the disclosure of Confidential Information, the receiving Party shall immediately inform the disclosing Party thereof in writing or in text form. The receiving Party shall further support the disclosing Party in its efforts to prevent the disclosure of the Confidential Information.

12.4 The obligation to maintain secrecy shall not apply if the Confidential Information was already known to the receiving Party prior to disclosure, is generally known or becomes known without fault of the receiving Party, was developed by the receiving Party itself without access to the Confidential Information of the disclosing Party or is brought to the attention of the third party by a bona fide third party authorized to do so. The mandatory statutory duties of disclosure shall remain unaffected. If the receiving Party invokes one or more of the aforementioned reasons, it must substantiate them by submitting suitable evidence.

12.5 The obligation to maintain secrecy shall commence upon knowledge of the Confidential Information and shall continue for the entire term of this Agreement. In addition, the obligation to maintain secrecy shall exist for a period of three years from termination or the end of the term of the contract, unless statutory provisions provide for a longer obligation to maintain secrecy. In particular, any business secrets shall be treated confidentially for as long as they are business secrets.

12.6 Insofar as agreed in the order form, mogenius shall be entitled to name Customer as a reference customer, stating the full company name and using the company logo in marketing materials (including websites).

12.7 With the exception of Section 12.6, the above provisions of this Section 12 do not establish any rights of use under intangible property law. All rights of use granted under this Agreement shall remain unaffected by the above Section 12.

13 Warranty

13.1 mogenius provides warranty for all Services provided free of charge in accordance with the statutory provisions.

13.2 mogenius shall provide warranty for defects in the provision of the Services exclusively in accordance with the following provisions and the Service Specification..

13.3 Defects are significant deviations from the contractually agreed functional scope of the Services.

13.4 If the Services to be provided by mogenius under this Agreement are defective, mogenius shall, within a reasonable period of time and after receipt of a written (e-mail sufficient) notice of defects from the Customer, either remedy the defects or provide the Services again, at its discretion. When using third-party software which mogenius has licensed for use by Customer, the remedy of defects shall consist of the procurement and installation of publicly available upgrades, updates or patches. The provision of workarounds allowing the Customer to reasonably circumvent defects and to use the Services in accordance with this Agreement shall also be deemed to be a remedy of defects.

13.5 If the defect-free provision of the Services fails for reasons for which mogenius is responsible, within a reasonable period of time set by the Customer in writing (e-mail sufficient), the Customer may reduce the agreed remuneration by a reasonable amount. The right to a reduction is limited to the amount of the monthly fixed price relating to the defective part of the Services.

13.6 If the reduction according to Section 13.5 in two consecutive months or in two months of a quarter reaches the maximum amount specified in Section 13.5, Customer may terminate the Agreement without notice.

13.7 Customer shall immediately notify mogenius of any defects in writing (e-mail sufficient). Furthermore, Customer shall reasonably support mogenius in the rectification of defects free of charge, including without limitation by providing mogenius with all information and documents reasonably necessary for the analysis and rectification of defects.

13.8 Notwithstanding Section 14, further warranty claims are excluded. In particular, any liability for initial defects according to Sec. 536a para. 1, 1st Alt. German Civil Code (*Bürgerliches Gesetzbuch, BGB*) is excluded.

13.9 The limitation period for warranty claims is one year, unless they are based on intent or gross negligence or relate to injury to life, body or health.

14 Liability

14.1 For Services provided free of charge, mogenius is liable in accordance with the statutory provisions.

14.2 mogenius shall be fully liable for intent and gross negligence and damages resulting from injury to life, body or health.

14.3 Other than the cases described in Section 14.2 above, mogenius is liable for slight negligence only in cases of a breach of a duty essential to the purposes of this Agreement. Duties are considered essential if necessary for the due execution of the Agreement so that Customer may generally rely on their proper observation. Such liability is limited to the typical and foreseeable damages at the time of conclusion of the Agreement.

14.4 The typical and foreseeable damages shall be limited to the Liability Cap set out in the order form.

14.5 Other than the cases described in Section 14.2 above, mogenius shall not be liable for any lack of commercial results, indirect damages and loss of profits.

14.6 The exclusions and limitations of liability of this Section shall apply accordingly in favour of the legal representatives (*gesetzliche Vertreter*), officers, employees, agents and assistants (*Erfüllungsgehilfen*) of mogenius and its subcontractors in case of a direct liability towards Customer.

14.7 Any liability of mogenius for guarantees (which must be expressly designated as such in order form or this Agreement to be deemed guarantees in the legal sense) and for claims under the German Product Liability Act (*Produkthaftungsgesetz*) remains unaffected.

14.8 Any further liability of mogenius for damages – irrespective of the legal grounds – shall be excluded.

15 Amendments to the Agreement

mogenius may amend this Agreement in accordance with this Section 15 with effect for the future, it there is a valid reason for such amendment and insofar as the amendment is reasonable taking into account the contractual balance between the Parties and both Parties' interests. A valid reason exists in particular if the amendment is necessary (i) to implement changed legal requirements, administrative orders or case law, (ii) to implement changed technical requirements, (iii) to maintain the operation of mogenius' Services, (iv) to adapt to changed market conditions, or (v) in favor of Customer. Except to the extent permitted in Section 4 of this Agreement, amending or changing a main performance obligation is excluded. mogenius shall inform Customer about an amendment at least six weeks in writing (text form or e-mail sufficient) or within the Services. Customer may object to the amendment. If Customer does not object within six weeks after receipt of the notification of the amendment, the amendments to the Agreement shall be deemed agreed between the Parties. mogenius shall inform Customer specifically about the six-week objection period and the legal consequences of Customer's silence as well as the effective date of the amendment in the notification of the amendment.

16 Miscellaneous

16.1 This Agreement (including the order form) includes the entire agreements of the Parties in respect of the subject matter hereof.

16.2 In case of conflicts or ambiguity in or between Sections and Annexes and Appendices of this Agreement, the provisions in the Annexes shall prevail.

16.3 Any amendments or supplements to this Agreement must be in writing (electronic form sufficient) in order to be legally effective. This shall also apply in respect of any waiver of the form requirement.

16.4 Customer may only offset claims of mogenius or assert a right of retention if the counterclaim is undisputed or recognized by declaratory judgment or is in a synallagmatic relationship to the claim in question.

16.5 Nothing in this Agreement and no action taken under this Agreement is intended to or shall operate to create a partnership, employment relationship or joint venture between the Parties, or to authorize either Party to act as agent for the other, and neither Party shall have authority to act in the name or on behalf of or otherwise to bind the other in any way, except where expressly stated otherwise in this Agreement.

16.6 Neither Party shall have the right to assign this Agreement or its rights or obligations hereunder to a third party without the prior written consent of the other Party.

16.7 This Agreement shall be exclusively governed by and construed in accordance with the substantive laws of Germany. The United Nations Convention on Contracts for the International Sale of Goods (CISG) shall not apply.

16.8 Exclusive place of jurisdiction for any disputes based on or in connection with this Agreement is Cologne, Germany.

Annex 1 – Data Processing Agreement

Attachment to the Terms of Service

Data Processing Agreement

between

a customer of the mogenius-Services or mogenius-Products

as Controller (hereinafter “**Controller**“),

and

mogenius GmbH, Heliosstr. 6a, 50825 Cologne

as Data Processor (hereinafter „**Data Processor**“,

Controller and Data Processor jointly the “**Parties**”)

Preamble

The Controller has commissioned the Data Processor in a contract already concluded (hereinafter referred to as the "**Main Contract**") for the services specified therein. Part of the execution of the contract is the processing of personal data. In particular, Art. 28 GDPR imposes specific requirements on such commissioned processing. To comply with these requirements, the Parties enter into the following Data Processing Agreement (hereinafter referred to as the “**Agreement**”), the performance of which shall not be remunerated separately unless expressly agreed.

§ 1 Definitions

(1) Pursuant to Art. 4 (7) GDPR, the Controller is the entity that alone or jointly with other Controllers determines the purposes and means of the processing of personal data.

(2) Pursuant to Art. 4 (8) GDPR, a Data Processor is a natural or legal person, authority, institution, or other body that processes personal data on behalf of the Controller.

(3) Pursuant to Art. 4 (1) GDPR, personal data means any information relating to an identified or identifiable natural person (hereinafter "**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(4) Personal data requiring special protection are personal data pursuant to Art. 9 GDPR revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of Data Subjects, personal data pursuant to Art. 10 GDPR on criminal convictions and criminal offenses or related security measures, as well as genetic data pursuant to Art. 4 (13) GDPR, biometric data pursuant to Art. 4 (14) GDPR, health data pursuant to Art. 4 (15) GDPR, and data on the sex life or sexual orientation of a natural person.

(5) According to Article 4 (2) GDPR, the processing is any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(6) Pursuant to Article 4 (21) GDPR, the supervisory authority is an independent state body established by a Member State pursuant to Article 51 GDPR.

§ 2 Subject of the contract

(1) The Data Processor provides the services specified in the Main Contract for the Controller. In doing so, the Data Processor obtains access to personal data, which the Data Processor processes for the Controller exclusively on behalf of and in accordance with the Controller's instructions. The scope and purpose of the data processing by the Data Processor are set out in the Main Contract and any associated service descriptions. The Controller shall be responsible for assessing the admissibility of the data processing.

(2) The Parties conclude the present Agreement to specify the mutual rights and obligations under data protection law. In case of doubt, the provisions of this Agreement shall take precedence over the provisions of the Main Contract.

(3) The provisions of this contract shall apply to all activities related to the Main Contract in which the Data Processor and its employees or persons authorized by the Data Processor come into contact with personal data originating from the Controller or collected for the Controller.

(4) The term of this Agreement shall be governed by the term of the Main Contract unless the following provisions give rise to further obligations or termination rights.

§ 3 Right of instruction

(1) The Data Processor may only collect, process or use data within the scope of the Main Contract and in accordance with the instructions of the Controller; this applies in particular with regard to the transfer of personal data to a third country or to an international organization. If the Data Processor is required to carry out further processing by the law of the European Union or the Member States to which it is subject, it shall notify the Controller of these legal requirements prior to the processing.

(2) The instructions of the Controller shall initially be determined by this Agreement. Thereafter, they may be amended, supplemented, or replaced by the Controller in writing or text form by individual instructions (Individual Instructions). The Controller shall be entitled to issue such instructions at any time. This includes instructions with regard to the correction, deletion, and blocking of data.

(3) All instructions issued shall be documented by the Controller. Instructions that go beyond the service agreed in the Main Contract shall be treated as a request for a change in service.

(4) If the Data Processor is of the opinion that an instruction of the Controller violates data protection provisions, it shall notify the Controller thereof without undue delay. The Data Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller. The Data Processor may refuse to carry out an obviously unlawful instruction.

§ 4 Types of data processed, group of Data Subjects

(1) Within the scope of the implementation of the Main Contract, the Data Processor shall have access to the personal data specified in more detail in **Annex 1**.

(2) The group of Data Subjects affected by the data processing is listed in **Annex 2**.

§ 5 Protective measures of the Data Processor

(1) The Data Processor shall be obliged to observe the statutory provisions on data protection and not to disclose information obtained from the Controller's domain to third parties or expose it to their access. Documents and data shall be secured against disclosure to unauthorized persons, taking into account the state of the art.

(2) The Data Processor shall organize the internal organization within its field of responsibility in such a way that it meets the special requirements of data protection. It shall have taken the technical and organizational measures specified in **Annex 3** to adequately protect the Controller's data pursuant to Art. 32 GDPR, which the Controller acknowledges as adequate. The Data Processor reserves the right to change the security measures taken while ensuring that the contractually agreed level of protection is not undercut.

(3) The persons employed in the data processing by the Data Processor are prohibited from collecting, processing or using personal data without authorization. The Data Processor shall oblige all persons entrusted by it with the processing and performance of this contract (hereinafter "**Employees**") accordingly (obligation of confidentiality, Art. 28 (3) lit. b GDPR) and shall ensure compliance with this obligation with due care.

(4) The Data Processor has appointed a data protection officer. The Data Processor's data protection officer is heyData GmbH, Gormannstr. 14, 10119 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Information obligations of the Data Processor

(1) In the event of disruptions, suspected data protection violations or breaches of contractual obligations of the Data Processor, suspected security-related incidents or other irregularities in the processing of personal data by the Data Processor, by persons employed by it within the scope of the contract or by third parties, the Data Processor shall inform the Controller without undue delay. The same shall apply to audits of the Data Processor by the data protection supervisory authority. The notification of a personal data breach shall contain at least the following information:

(a) a description of the nature of the personal data breach, including, to the extent possible, the categories and the number of Data Subjects affected, the categories affected and the number of personal data records affected;

(b) a description of the measures taken or proposed by the Data Processor to address the breach and, where applicable, measures to mitigate its possible adverse effects;

(c) a description of the likely consequences of the personal data breach.

(2) The Data Processor shall immediately take the necessary measures to secure the data and to mitigate any possible adverse consequences for the Data Subjects, inform the Controller thereof and request further instructions.

(3) In addition, the Data Processor shall be obliged to provide the Controller with information at any time insofar as the Controller's data are affected by a breach pursuant to paragraph 1.

(4) The Data Processor shall inform the Controller of any significant changes to the security measures pursuant to Section 5 (2).

§ 7 Control rights of the Controller

(1) The Controller may satisfy itself of the technical and organizational measures of the Data Processor prior to the commencement of data processing and thereafter regularly on a quarterly basis. For this purpose, the Controller may, for example, obtain information from the Data Processor, obtain existing certificates from experts, certifications or internal audits or, after timely coordination, personally inspect the technical and organizational measures of the Data Processor during normal business hours or have them inspected by a competent third party, provided that the third party is not in a competitive relationship with the Data Processor. The Controller shall carry out checks only to the extent necessary and shall not disproportionately disrupt the operations of the Data Processor in the process.

(2) The Data Processor undertakes to provide the Controller, upon the latter's verbal or written request and within a reasonable period of time, with all information and evidence required to carry out a check of the technical and organizational measures of the Data Processor.

(3) The Controller shall document the results of the inspection and notify the Data Processor thereof. In the event of errors or irregularities which the Controller discovers, in particular during the inspection of the results of the inspection, the Controller shall inform the Data Processor without undue delay. If facts are found during the control, the future avoidance of which requires changes to the ordered procedure, the Controller shall notify the Data Processor of the necessary procedural changes without delay.

§ 8 Use of service providers

(1) The contractually agreed services shall be performed with the involvement of the service providers named in **Annex 4** (hereinafter "**Sub-processors**"). The Controller grants the Data Processor its general authorization within the meaning of Article 28 (2) s. 1 GDPR to engage additional Sub-processors within the scope of its contractual obligations or to replace Sub-processors already engaged.

(2) The Data Processor shall inform the Controller in advance by e-mail newsletter of any intended change regarding the involvement or replacement of a Sub-processor. The email newsletter will be received by the Controller after sending an email with the subject "Subscribe" to info@mogenius.com. The Controller may object to an intended enlistment or substitution of a Sub-processor for good cause under data protection law.

(3) The objection to the intended involvement or replacement of a Sub-processor must be raised within 2 weeks of the information being sent in the email newsletter. If no objection is raised, the involvement or replacement shall be deemed approved. If there is a good cause under data protection law and a mutually agreeable solution cannot be found between the Controller and Data Processor, the Controller shall have a special right of termination at the end of the month following the objection.

(4) When engaging Sub-processors, the Data Processor shall oblige them in accordance with the provisions of this Agreement.

(5) A Sub-processor relationship within the meaning of these provisions does not exist if the Data Processor commissions third parties with services that are regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services without any specific reference to services provided by the Data Processor to the Controller and guarding services. Maintenance and testing services constitute Sub-processor relationships requiring consent insofar as they are provided for IT systems that are also used in connection with the provision of services for the Controller.

§ 9 Requests and rights of Data Subjects

(1) The Data Processor shall support the Controller with suitable technical and organizational measures in fulfilling the Controller's obligations pursuant to Articles 12-22 and 32 to 36 GDPR.

(2) If a Data Subject asserts rights, such as the right of access, correction or deletion with regard to his or her data, directly against the Data Processor, the latter shall not react independently but shall refer the Data Subject to the Controller and await the Controller's instructions.

§ 10 Liability

(1) In the internal relationship with the Data Processor, the Controller alone shall be liable to the Data Subject for compensation for damage suffered by a Data Subject due to inadmissible or incorrect data processing under data protection laws or use within the scope of the commissioned processing.

(2) The Data Processor shall have unlimited liability for damage insofar as the cause of the damage is based on an intentional or grossly negligent breach of duty by the Data Processor, its legal representative or vicarious agent.

(3) The Data Processor shall only be liable for negligent conduct in the event of a breach of an obligation, the fulfillment of which is a prerequisite for the proper performance of the contract and the observance of which the Controller regularly relies on and may rely on, but limited to the average damage typical for the contract. In all other respects, the liability of the Processor - including for its vicarious agents - shall be excluded.

(4) The limitation of liability pursuant to § 10.3 shall not apply to claims for damages arising from injury to life, body, health or from the assumption of a guarantee.

§ 11 Termination of the Main Contract

(1) After termination of the Main Contract, the Data Processor shall return to the Controller all documents, data and data carriers provided to it or - at the request of the Controller, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany - delete them. This shall also apply to any data backups at the Data Processor. The Data Processor shall on request provide documented proof of the proper deletion of any data.

(2) The Controller shall have the right to control the complete and contractual return or deletion of the data at the Data Processor in an appropriate manner.

(3) The Data Processor shall be obligated to keep confidential the data of which it has become aware in connection with the Main Contract even beyond the end of the Main Contract. The present Agreement shall remain valid beyond the end of the Main Contract as long as the Data Processor has personal data at its disposal which have been forwarded to it by the Controller or which it has collected for the Controller.

§ 11 Final provisions

(1) Amendments and supplements to this Agreement must be made in writing. This shall also apply to any waiver of this formal requirement. The priority of individual contractual agreements shall remain unaffected.

(2) If individual provisions of this Agreement are or become wholly or partially invalid or unenforceable, this shall not affect the validity of the remaining provisions.

(3) This agreement is subject to German law.

Annex

Annex 1 - Description of the data/data categories

Names, email addresses, IP addresses, phone numbers, addresses, business addresses

Annex 2 - Description of affected Data Subject/groups of affected Data Subjects

Controllers, employees of controllers, third parties

Annex 3 - Technical and organizational measures of the Data Processor

1. This attachment summarizes the technical and organizational measures of mogenius GmbH.

2. Confidentiality (art. 32 para. 1 lit. b GDPR)

2.1 Access control

The following implemented measures prevent unauthorized persons from gaining access to the data processing facilities:

- Alarm system
- Chip card/transponder locking system

2.2 Access control

The following implemented measures prevent unauthorized persons from gaining access to the data processing systems:

- Authentication with user and password
- Use of firewalls
- Encryption of data carriers
- Encryption of notebooks / tablets
- Management of user authorizations
- Use of 2-factor authentication

2.3 Access control

The following implemented measures ensure that unauthorized persons do not have access to personal data:

- Management of user rights by system administrators

2.4. separation control

The following measures ensure that personal data collected for different purposes are processed separately:

- Encryption of data sets processed for the same purpose.

3. Integrity (Art. 32 Par. 1 lit. b GDPR)

3.1 Transfer control

It is ensured that personal data cannot be read, copied, modified or removed without authorization during transmission or storage on data carriers and that it is possible to verify which persons or bodies have received personal data. The following measures are implemented to ensure this:

- WLAN encryption (WPA2 with strong password)
- Provision of data via encrypted connections such as SFTP or HTTPS

3.2 Input control

The following measures ensure that it is possible to check who has processed personal data in data processing systems and at what time:

- Traceability of input, modification and deletion of data through individual user names (not user groups).

4. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client:

- Fire extinguishers in server rooms
- Fire and smoke detection systems
- Devices for monitoring temperature and humidity in server rooms
- Air conditioning in server rooms
- Protective socket strips in server rooms
- Uninterruptible power supply (UPS)
- Data protection safe
- Video surveillance in server rooms
- Alarm notification in case of unauthorized access to server rooms
- Regular backups

5. Procedures for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR)

5.1 Data Protection Management

The following measures are intended to ensure that an organization that meets the basic requirements of data protection law is in place:

- Use of the heyData platform for data protection management
- Appointment of the data protection officer heyData
- Obligation of employees to maintain data secrecy
- Regular training of employees in data protection
- Keeping an overview of processing activities (Art. 30 GDPR)
- Conducting data protection impact assessments, if required (Art. 35 GDPR).

5.2 Incident Response Management

The following measures are intended to ensure that notification processes are triggered in the event of data protection breaches:

- Notification process for data protection breaches pursuant to Art. 4 No. 12 GDPR vis-à-vis the supervisory authorities (Art. 33 GDPR).
- Notification process for data protection breaches pursuant to Art. 4 No. 12 GDPR vis-à-vis the data subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data mishaps
- Use of firewalls

5.3 Data protection-friendly default settings (Art. 25 (2) GDPR)

The following implemented measures take into account the requirements of the "Privacy by design" and "Privacy by default" principles:

- Training of employees in "Privacy by design" and "Privacy by default".
- No more personal data is collected than is necessary for the respective purpose.

5.4 Order control

The following measures ensure that personal data can only be processed in accordance with instructions:

- Written instructions to the contractor or instructions in text form (e.g. by order processing contract).
- Ensuring that data is destroyed after completion of the order, e.g. by requesting appropriate confirmations
- Confirmation from contractors that they commit their own employees to data secrecy (typically in the order processing contract)
- Careful selection of contractors (especially with regard to data security)

Annex 4 – Current subcontractors

- Microsoft Azure (Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA), function: data hosting, server location: EU
- SendGrid (Twilio, Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105, USA), function: Email dispatch, server location: USA
- Stripe (Stripe Inc., 510 Townsend Street, San Francisco, CA 94103, USA), function: payment processor, server location: USA
- Cloudflare (Cloudflare Inc., 106 East 6th Street, Suites 350 and 400, Austin, TX 78701, USA), function: CDN, Web Application Firewall, DDoS protection, server location: Europe/USA