



# Engagement Letter

## 1. General Terms

- 1.1. This engagement letter (“**Agreement**”) sets forth the terms and conditions under which Maetzler Rechtsanwalts GmbH & Co KG, a company registered under FN 502860a with the companies register of the Vienna commercial court, Schellinggasse 3/10, 1010 Vienna, Austria, (“**GDPR-Rep.eu**”) provides the services as a representative according to Art 27 GDPR and the software as a service (“**SaaS**”) available at [www.gdpr-rep.eu](http://www.gdpr-rep.eu) for companies without an establishment in the EU (“**Client**”).
- 1.2. Subject of the Agreement are the following basic services as a representative according to Art 27 GDPR:
  - Art. 27 GDPR compliant representative located in Europe acting as a one-stop-shop in all EU-Member States;
  - privacy landing page for Clients, which can be individualized with the Client’s logo;
  - a DSR management tool to structure privacy requests and handle these from a formal point of view, including a request management workflow;
  - unlimited forwarding of electronic requests from data subjects;
  - unlimited forwarding of postal messages from data subjects;
  - unlimited forwarding of requests from supervisory authorities;
  - a Client login for a dashboard to manage all privacy requests and the subscription;
  - the information to include in the Client’s privacy policy regarding the appointment of GDPR-Rep.eu as representative;
  - certificate for appointing GDPR-Rep.eu as the Client’s representative, which the Client can include in its website.
  - the maintenance of the record of processing activities under the responsibilities of the controller(together “**Basic GDPR-Rep.eu Services**”).
- 1.3. This Agreement, the Power of Attorney (“**PoA**”) signed by the Client to appoint GDPR-Rep.eu as representative according to Art 27 GDPR and separate price information

constitute the whole agreement. Contradicting terms and conditions of Clients do not apply. Oral agreements or further written agreements do not exist. Therefore, the Agreement, the PoA and separate price information form the entire agreement and understanding of the parties with respect to the Basic GDPR-Rep.eu Services and supersede all prior or contemporaneous understandings regarding such subject matter. Should the Client requests bespoke advisory or consulting services GDPR-Rep.eu or Maetzler Rechtsanwalts GmbH & Co KG will provide the Client with the terms and condition for this additional scope.

1.4. All services of GDPR-Rep.eu are addressed to businesses only and not to consumers.

## 2. Definitions

As used in this Agreement, the terms defined below in this Section 2 shall have the meanings set forth below:

Agreement	means this agreement between the GDPR-Rep.eu and the Client.
Basic GDPR-Rep.eu Service	means the services listed in 1.2 excluding any other services, especially excluding individual bespoke services, answering requests of data subjects and authorities, drafting and maintaining documentation obligatory according to GDPR (e.g. privacy policy, records of processing activities, data protection impact assessment, consent management, data processing agreements, etc.)
Client	means any business client who has signed the PoA
Controller	means in accordance with Art 4 para 7 GDPR the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law
DPA	means Data Processor Agreement which governs the processing of data subject's data by GDPR-Rep.eu as Processor for the Client as Controller and which is attached as Annex 1.
DSR	means data subject request as a general term for rights of data subjects according to Art 13-22 GDPR.
GDPR	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
GDPR-Rep.eu	means Maetzler Rechtsanwalts GmbH & Co KG, a company registered under FN 502860a with the

	companies register of the Vienna commercial court, 1010 Vienna, Austria.
License	means the rightful use of the provided Basic GDPR-Rep.eu Service complying with the terms and conditions of this Agreement
Platform	means the website including the login section available at <a href="http://www.gdpr-rep.eu">www.gdpr-rep.eu</a> .
PoA	means the Power of Attorney signed by the Client to appoint GDPR-Rep.eu as representative according to Art 27 GDPR.
Privacy Policy	Means the information according to Art 13 or 14 GDPR.
Processor	means in accordance with Art 4 para 8 GDPR a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
SaaS	means software as a service available at <a href="http://www.gdpr-rep.eu">www.gdpr-rep.eu</a> .
Tax	means VAT, other tax, duty, fee or any kind of charges as applicable that is imposed by any government or any tax authority.
VAT	means value added tax.

### 3. Scope of Work

- 3.1. GDPR-Rep.eu shall have the right and the obligation to represent the Client as a representative according to GDPR. The detailed list of the Basic GDPR-Rep.eu Services is included in 1.2.
- 3.2. Individual bespoke legal services, especially answering requests of data subjects and authorities, drafting and maintaining documentation obligatory according to GDPR (e.g. privacy policy, records of processing activities, data protection impact assessment, consent management, data processing agreements, etc.), advisory or consulting services as well as additional services and features developed in the future are not included in the Basic GDPR-Rep.eu Services and therefore not in the scope of this Agreement. Nevertheless Maetzler Rechtsanwalts GmbH & Co KG may provide individual legal advice upon written request of the Client and offers 15% discount on privacy related legal advice for a number of billable hours depending on the plan the Client subscribes to (see 4.1). The standard hourly rates are at the moment EUR 350 for attorneys and EUR 270 for associates.
- 3.3. The Client acknowledges that GDPR-Rep.eu shares all information on the processing of data, especially the appointment of GDPR-Rep.eu as the Client's representative, the Privacy Policy as applicable or the record of processing activities upon request with supervisory authorities and data subjects, if they have a right according to GDPR to request such document.

- 3.4. Should data subjects contact the Client via the contact form provided by GDPR-Rep.eu, GDPR-Rep.eu processes these data as Processor for the Client who is Controller. In such case the processing of data is governed by the DPA (Annex 1).

#### **4. Available Plans**

- 4.1. The applicable plan for Basic GDPR-Rep.eu Services depend on the size of the company. The size of the company is defined according to the Eurostat categories and therefore by the number of persons employed. Persons employed includes employees but also working proprietors, partners working regularly in the enterprise and unpaid family workers. The available plans currently are:

- EUR 19/month for Start-ups (meaning founding teams without employees); discount according to 3.2 for 3 hours per month;
- EUR 39/month for Micros (meaning companies with under 10 persons employed); discount according to 3.2 for 4 hours per month;
- EUR 79/month for small companies (meaning companies with 10 to 49 persons employed); discount according to 3.2 for 5 hours per month;
- EUR 189/month for mid-sized companies (meaning companies with 50 to 249 persons employed); discount according to 3.2 for 8 hours per month;

The pricing for large companies (meaning companies with 250+ persons employed) is set individually taking into account the company size, the countries the Client operates in, the types of data processed and especially the data privacy sensitivity of the Client's business model.

- 4.2. If the Client chooses instead of a monthly payment a quarterly payment, the prices listed in 4.1 are reduced by 3%. If the Client chooses instead of a monthly payment a yearly payment, the prices listed in 4.1 are reduced by 5%.
- 4.3. To which package the Client subscribes depends on information on the Client's company size provided by the Client during the onboarding process. Should the information provided by the Client be or become incorrect (e.g. by the Client's growth or downsize regarding the number of persons employed) and classified in another category of companies, GDPR-Rep.eu is entitled to amend the fees and charge the Client the monthly fee for the category of companies the Client falls under.
- 4.4. The prices valid at a special point in time are published on GDPR-Rep.eu's website. The individual price is shown to the Client before payment is proceeded. The fees are subject to changes from time to time.
- 4.5. All fees are exclusive of value added tax (or similar tax) ("**VAT**"), other tax, duty, fee or any kind of charges as applicable that is imposed by any government or any tax authority

(together “**Tax**”). If certain expenses such as, translation costs, postal charges or travel expenses occur, these expenses will be charged in addition at cost and with the Client’s prior written approval, together with any applicable Tax.

- 4.6. Unless otherwise agreed, the Basic GDPR-Rep.eu Services are invoiced on a monthly basis.

## **5. Client’s Cooperation and Undertakings**

- 5.1. The Client is aware that it is obliged to:

- 5.1.1. provide the data subject at the time when personal data are obtained with all information listed in Art 13 or 14 GDPR as applicable;
- 5.1.2. maintain a record of processing activities under its responsibility according to Art 30 GDPR;
- 5.1.3. comply with the obligation stipulated in GDPR when processing data of data subjects in the EU.

- 5.2. The Client undertakes to

- 5.2.1. provide GDPR-Rep.eu with the information necessary according to Art 13 or 14 GDPR and with its record of processing activities;
- 5.2.2. take care of all requests addressed to GDPR-Rep.eu on behalf of the Client;
- 5.2.3. inform itself on the relevant data protection provisions in the EU-countries it is addressing customers or monitoring data subjects.

- 5.3. The Client agrees to be mentioned as a reference Client on GDPR-Rep.eu’s website and in other means of communication and advertising and to the usage of its logo for this purpose.

## **6. Intellectual Property**

The Client has the right to use documents and tools provided by GDPR-Rep.eu for purposes of Basic GDPR-Rep.eu Services and legitimate ancillary purposes. For all other purposes any use of documents or tools requires GDPR-Rep.eu’s prior written consent. Without express agreement to the contrary, GDPR-Rep.eu does not transfer any intellectual property rights, including copyright, in any documents, software or other tools or materials provided to the Client.

## **7. Liability**

- 7.1. The aggregate liability of GDPR-Rep.eu (including the liability of its owners, shareholders, managing directors, employees, associated lawyers, subcontractors and affiliated companies) vis-à-vis the Client for all damages, losses, expenses and other disadvantages suffered as a result of any GDPR-Rep.eu's services, or in connection with GDPR-Rep.eu's advice shall be limited to EUR 400,000 (Euro four hundred thousand).
- 7.2. GDPR-Rep shall not be liable for damages, losses, expenses or other disadvantages caused as a result of slight negligence.
- 7.3. GDPR-Rep.eu shall only be liable to the Client but not to any third parties.
- 7.4. GDPR-Rep.eu is not liable for any non-compliance of GDPR or any other data protection law by the Client. GDPR-Rep.eu does furthermore not qualify as responsible person ("*Verantwortlicher*" according to Section 9 Austrian VStG). Therefore GDPR-Rep.eu is not liable for
  - any damages or whatever compensation claimed by third parties
  - or fines or penalties imposed by authorities

arising from the non-compliance with GDPR or any other data protection law by the Client and the Client will hold GDPR-Rep.eu harmless for any such claims from third parties or fines and penalties imposed by authorities on the Client or GDPR-Rep.eu on behalf of the Client.

## **8. Term and Termination**

- 8.1. The Agreement enters into force with signing the PoA by the Client. It is entered for an unlimited period of time.
- 8.2. The Client may terminate this engagement at any time by written notice (including electronical communication) to GDPR-Rep.eu without stating reasons for the termination. The termination will become effective at the end of the payment period the Client chooses during the onboarding. If the Client chooses a monthly payment, the termination becomes effective at the end of the following month. If the Client chooses quarterly or yearly payment the termination becomes effective at the end of the quarter or year the Client gives termination notice at least one month ahead.
- 8.3. GDPR-Rep.eu may terminate this engagement at any time by written notice (including electronical communication) to the Client without stating reasons for the termination. The termination becomes effective at the end of the following month GDPR-Rep.eu gives termination notice to the Client.
- 8.4. Upon termination of the Agreement by either party for any reason, GDPR-Rep.eu's fees and expenses immediately become due and payable by the Client, including the fees and

expenses of any third party retained by GDPR-Rep.eu, including any Tax applicable to such amounts, incurred up to the date of termination.

## **9. Miscellaneous**

### **9.1. Tax**

The Client shall economically bear all Taxes becoming due because of rendering Basic GDPR-Rep.eu Services, except income tax imposed on GDPR-Rep.eu.

### **9.2. Electronic Notice**

GDPR-Rep.eu may provide Clients with information and notices about services electronically, including via email or through the GDPR-Rep.eu portal. Notice is given as of the date it is made available by GDPR-Rep.eu.

### **9.3. Severance**

If any provision of this agreement is or becomes ineffective, the effectiveness of the remaining provisions shall not be affected. In such case, an ineffective provision shall be construed to be replaced by a provision that comes closest to the economic and legal aim of such ineffective provision.

### **9.4. Governing Law**

This Agreement shall be governed by and construed in accordance with the Laws of the Republic of Austria, with the exception of the UN Sale Convention and the conflict of law rules.

### **9.5. Jurisdiction**

Any and all disputes arising out of or in connection with this Agreement, including, without limitation, a dispute as to its violation or the conclusion, validity, nullity, existence, termination or dissolution of this Agreement, shall be finally and exclusively resolved and settled by the competent courts for the first Vienna district.

## DATA PROCESSOR AGREEMENT

### 1. Introduction

- 1.1 This agreement regarding processing of personal data ("**DPA**") regulates GDPR-Rep.eu's (the "**Processor**") processing of personal data on behalf of the Client ("**Controller**") and is attached as an addendum to the Engagement Letter in which the parties have agreed the terms for the Processor's delivery of Basic GDPR-Rep.eu Services to the Controller.

### 2. Legislation

- 2.1. The DPA shall ensure that the Processor complies with the applicable data protection and privacy legislation ("**Applicable Law**"), including in particular GDPR.

### 3. Processing of personal data

- 3.1. **Purpose:** The purpose of the processing under the Engagement Letter is the provision of the GDPR-Rep.eu's services by the Processor as specified in the Engagement Letter.
- 3.2 In connection with the Processor's delivery of GDPR-Rep.eu's services to the Controller, the Processor will process the Controller's and his customer's personal data on behalf of the Data Controller.
- 3.3 "Personal data" includes "*any information relating to an identified or identifiable natural person*" as defined in Art 4 (1) (1) GDPR (the "**Personal Data**"). The categories and types of Personal Data processed by the Processor on behalf of the Controller are listed in sub-appendix A. The Processor only performs processing activities that are necessary and relevant to perform GDPR-Rep.eu's services. The parties shall update sub-appendix A whenever changes occur that necessitates an update.

### 4. Instruction

- 4.1 The Processor may only act and process the Personal Data in accordance with its function as representative according to Art 27 GDPR and with the documented instruction from the Controller ("**Instruction**"), unless required by law to act without such instruction. The Instruction at the time of entering into this DPA is that the Processor may only process the Personal Data with the purpose of delivering the GDPR-Rep.eu's services as described in the Engagement Letter.
- 4.2 The Controller guarantees to process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. The Controller's instructions for the processing of Personal Data shall comply with Applicable Law. The Controller will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which it was obtained.



4.3 The Processor will inform the Controller of any instruction that it deems to be in violation of Applicable Law and will not execute the instructions until they have been confirmed or modified.

## **5. The Processor's obligations**

### **5.1 Confidentiality**

5.1.1 The Processor shall treat all the Personal Data as strictly confidential information. The Personal Data may not be copied, transferred or otherwise processed in conflict with the Instruction, unless the Controller in writing has agreed.

5.1.2 The Processor's employees shall be subject to an obligation of confidentiality that ensures that the employees shall treat all the Personal Data under this DPA with strict confidentiality.

5.1.3 Personal Data will only be made available to personnel that require access to such Personal Data for the delivery of the GDPR-Rep.eu's services and this DPA.

5.2 The Processor shall also ensure that employees processing the Personal Data only process the Personal Data in accordance with the Instruction.

### **5.3 Security**

5.3.1 The Processor shall implement the appropriate technical and organizational measures in accordance with Art 32 GDPR. The security measures are subject to technical progress and development. The Processor may update or modify the security measures from time-to-time provided that such updates and modifications do not result in the degradation of the overall security.

5.4 The Processor shall provide documentation for the Processor's security measures if requested by the Controller in writing.

### **5.5 Data protection impact assessments and prior consultation**

If the Processor's assistance is necessary and relevant upon the Controller's prior written consent, the Processor shall assist the Controller in preparing data protection impact assessments in accordance with Art 35 GDPR, along with any prior consultation in accordance with Art 36 GDPR. The Processor would charge such assistance based on the hourly rate then applicable.

### **5.6 Rights of the data subjects**

5.6.1 If the Controller receives a request from a data subject for the exercise of the data subject's rights under the Applicable Law and the correct and legitimate reply to such a request necessitates the Processor's assistance upon the Controller's prior written consent, the Processor shall assist the Controller by providing the necessary information and documentation. The Processor shall be given reasonable time to assist the Controller with such requests in accordance with the Applicable Law.

5.6.2 If the Processor receives a request from a data subject for the exercise of the data subject's rights under the Applicable Law and such request is related to the Personal Data of the Controller, the Processor must immediately forward the request to the Data Controller and must refrain from responding to the person directly.

## 5.7 Personal Data Breaches

5.7.1 The Processor shall give immediate notice to the Controller if a breach occurs, that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, personal data transmitted, stored or otherwise processed regarding the Personal Data processed on behalf of the Controller ("**Personal Data Breach**").

5.7.2 The Processor shall make reasonable efforts to identify the cause of such a breach and take those steps as they deem necessary to establish the cause, and to prevent such a breach from reoccurring.

## 5.8 Documentation of compliance and Audit Rights

5.8.1 Upon request by a Controller, the Processor shall make available to the Controller all relevant information necessary to demonstrate compliance with this DPA. If the Controller requests an audit, the Processor will conduct an audit by IT security specialists and make the report available to the Controller. As the Processor is a law firm and obliged to professional confidentiality the Controller has no right to conduct an audit on its own.

## 5.9 Data Transfers

5.9.1 Subject to the GDPR-Rep.eu's services is the transfer of Personal Data to countries outside the European Economic Area. As far as the Processor processes Personal Data in its sphere only those storage solutions that provide secure services with adequate relevant safeguards will be employed.

## 6. Sub-Processors

6.1 The Data Processor is given general authorization to engage third-parties to process the Personal Data ("**Sub-Processors**") without obtaining any further written, specific authorization from the Controller, provided that the Processor notifies the Controller in writing about the identity and role of a potential Sub-Processor (and its processors, if any). If the Controller wishes to object to the relevant Sub- Processor, the Controller shall give notice hereof in writing within ten (10) business days from receiving the notification from the Processor. Absence of any objections from the Controller shall be deemed as a consent to the relevant Sub-Processor.

6.2 In the event the Controller objects to a new Sub-Processor and the Processor cannot accommodate the Controller's objection, the Controller may terminate the services by providing written notice to the Processor.

6.3 The Processor shall complete a written sub-processor agreement with any Sub-Processors. Such an agreement shall at minimum provide the same data protection

obligations as the ones applicable to the Processor, including the obligations under this DPA. The Processor shall on an ongoing basis monitor and control its Sub- Processors' compliance with the Applicable Law. Documentation of such monitoring and control shall be provided to the Controller if so requested in writing.

6.4 The Processor is accountable to the Controller for any Sub-Processor in the same way as for its own actions and omissions.

6.5 The Processor is at the time of entering into this DPA using the Sub- Processors listed in sub-appendix B. If the Processor initiates sub-processing with a new Sub-Processor, such new Sub-Processor shall be added to the list in sub-appendix B under paragraph 2.

## **7. Remuneration and costs**

7.1 Subject to 5.8.1 of this Data Processing Agreement the Controller shall remunerate the Data Processor based on time spent to perform the obligations under section 5.5, 5.6, 5.7 and 5.8 of this DPA based on the Processor's hourly rates then applicable. The current hourly rates are listed under point 3.2 of the Engagement letter.

7.2 The Processor is also entitled to remuneration for any time and material used to adapt and change the processing activities in order to comply with any changes to the Controller's Instruction, including implementation costs and additional costs required to deliver the GDPR-Rep.eu's services due to the change in the Instruction. The Processor is exempted from liability for non-performance with the Engagement Letter if the performance of the obligations under the Engagement Letter would be in conflict with any changed Instruction or if contractual delivery in accordance with the changed Instruction is impossible. This could for instance be the case; (i) if the changes to the Instruction cannot technically, practically or legally be implemented; (ii) where the Controller explicitly requires that the changes to the Instruction shall be applicable before the changes can be implemented; and (iii) in the period of time until the Engagement Letter is changed to reflect the new Instruction and commercial terms thereof.

## **8. Limitation of Liability**

8.1 The total aggregate liability to the Client, of whatever nature, whether in contract, tort or otherwise, of the Processor for any losses whatsoever and howsoever caused arising from or in any way connected with this engagement shall be subject to the "Limitation of Liability" clause set out in the Engagement Letter.

8.2 Nothing in this DPA will relieve the processor of its own direct responsibilities and liabilities under the GDPR.

## **9. Duration**

The DPA shall enter into force in case of a data subjects request via the Processor and only for such a processing of Personal Data. The Processor is not processing Personal Data of data subjects in the EU for any other purpose. Therefore, this DPA is only valid

for the limited period of time when the Processor is processing Personal Data of data subjects inside the EU.

#### **10. Termination**

Following expiration or termination of the Agreement, the Processor will delete or return to the Controller all Personal Data in its possession as provided in the Agreement except to the extent the Processor is required by Applicable law to retain some or all of the Data (in which case the Processor will archive the data and implement reasonable measures to prevent the Personal Data from any further processing). The terms of this DPA will continue to apply to such Personal Data.

#### **12. Contact**

The contact information for the Processor and the Controller is provided in the PoA.

## **Sub-appendix A**

### **1. Personal Data**

1.1 The Processor processes the following types of Personal Data in connection with its delivery of GDPR-Rep.eu's services:

Information on data subject using means provided by the Processor to address the Controller on all issues related to the Controller's processing, for the purposes of ensuring compliance with GDPR, especially:

1. Name, pseudonym or any other identification
2. Contact details such as postal address, email address and phone number
3. Any other Personal Data the data subject may include in or attach to a message to the Controller
4. Geolocation identified by the IP Addressee, for the sole purpose of validating the legitimacy of the request

### **2. Categories of data subjects**

2.1 The Processor processes personal data about the following categories of data subjects on behalf of the Controller:

1. data subjects inside the EU who are customers of the Controller(s) customer(s) that offer goods or services, irrespective of whether a payment of the data subject is required,
2. data subjects the Controller monitors as far as the monitored behavior takes place within the Union;

## **Sub-appendix B**

### **1. APPROVED SUB-PROCESSORS**

1.1 The following Sub-Processors shall be considered approved by the Controller at the time of entering into this Agreement:

- i. Digital Ocean
- ii. World4You (Email processing)
- iii. Microsoft

### **2. New Sub-Processors**

2.1 The following Sub-Processors have been added and communicated to the Data Controller prior to the relevant sub-processing: