my.WAGILE.pro
GDPR COMMISSIONED PROCESSING DOCUMENT

This document specifies the obligations of the Parties who entered into the Master Service Agreement concerning the data protection on commissioned processing within the meaning of Article 28 (3) of the GDPR.

It applies to all activities in connection with the Agreement and the processing of the customers personal data (hereinafter referred to as “Data”) by the employees of the Provider or persons commissioned by the Provider.

1. General information

The Service provided by the Provider to the Customer is specified in the Master Service Agreement and related Annexes. The Agreement specifies the subject matter as well as the duration of the commission along with the nature and purpose of the processing. The term of the Annex is based on the term of the Agreement, provided that the provisions of the Annex do not give rise to other obligations in excess hereof.

2. Scope and Responsibility

On behalf of the Customer for the purpose of the Master Service Agreement and to the extent stated therein, the Provider shall process the Data specified in Annex A.

In regards to this Agreement, in particular for the legality of data transfer to the Provider and for the legality of data processing (“Responsible Person” within the meaning of Article 4(7) of the GDPR), the Customer shall be solely responsible for compliance with the legal provisions of data protection laws. The Customer is responsible to get the agreement from the impacted people and to comply with GDPR before any transfer of any personal data on the Provider platforms or to use the Providers service.

The instructions shall be initially defined in the Master Service Agreement. These may further be supplemented, modified, or replaced by the Customer in writing or in an electronic format (text form). The new instructions shall be sent to the person designated by the Provider for verification and agreement. Instructions that are not provided for in the Master Service Agreement shall be treated as a request for a change in service. The Customer shall immediately follow up on verbal instructions in text form or in writing.

3. The Providers Obligations

Within the scope of the commission and on the instructions of the Customer, the Provider may only process Data of the data subjects unless there is an exceptional case within the meaning of Article 28(3)(a) of the GDPR. If the Provider believes that an instruction violates applicable laws, the Provider shall inform the Customer immediately. Until the instruction has been confirmed or amended by the Customer, the Provider may suspend the implementation of the instruction and the Service.

The internal organization of the Provider will be structured in such a way that it meets the special requirements of data protection. Technical and organizational measures shall be taken by the Provider that meet the requirements of the General Data Protection Regulation (Article 32 of the GDPR) to protect the Customer’s Data in an adequate way that ensures the confidentiality, availability, integrity and resilience of the services and systems in connection with the processing in the long term. The Customer may request to be made aware of these measures to ensure they offer an acceptable level of protection.

In Annex B, the measures taken by the Provider are described in more detail. The measures shall be subject to technical progress and further development/improvement in the future. In this respect, the Provider shall be permitted to implement improvements or alternative adequate measures at any time. The security level of the defined measures shall stay at the same level or improve but not be undershot. Major amendments shall be documented.

The Provider shall support the Customer, within the scope of its commercially reasonable possibilities, and to the extent agreed, in satisfying the requests and claims of data subjects pursuant to Chapter III of the GDPR and in complying with the obligations set out in Articles 33 to 36 of the GDPR.

The Provider guarantees that the employees and other persons working for the Provider which are involved in processing the Customer's Data are prohibited from processing the Data outside of the instructions. Next to this, the Provider guarantees that employees and the respective persons have undertaken to maintain confidentiality or are subject to an appropriate statutory obligation of confidentiality. The confidentiality obligation shall continue to apply even after the completion of the commission.

Any breaches of the Customer's personal Data protection must be announced by the Provider to the Customer with immediate effect. The Provider shall mitigate possible adverse consequences for the data subjects and take the necessary measures to secure the Data, and shall consult with the Customer without delay.

In case of any Data protection issues, the Data Protection Officer can be reached via email: suppport@wagile.pro with the subject "DATA PROTECTION ISSUE"

To comply with its obligations under Article 32(1)(d) of the GDPR, the Provider shall implement a procedure for a regular review. During the review the effectiveness of the organizational and technical measures so as to ensure the security of the processing may be reviewed. The Provider shall delete or correct the contractual Data if this is instructed by the Customer and included in the Master Service Agreement. Should the corresponding restriction of Data processing be impossible or impact conformity with Data protection legislation, the Provider shall return these Data carriers to the Customer, unless already agreed in the Master Service Agreement or undertake the deletion or destruction of Data carriers and other materials in conformity with Data protection on the basis of a specific assignment by the Customer. In special cases, these shall be retained or handed over, but to be determined by the Customer. Unless already agreed in the Master Service Agreement, the compensation and protective measures for these purposes shall be agreed separately.

Following the completion of the commission, Data carriers, Data and all other materials shall either be deleted or surrendered at the request of the Customer. The related and additional costs arising due to deviating specifications in the deletion or surrender of the Data shall be charged to and borne by the Customer.

In case of any claims by a Data subject under the Article 82 of the GDPR against the Customer, the Provider shall undertake to support the Customer in defending the claim within the scope of its reasonably commercial possibilities.

According to its current hourly rates or external expenses, the Provider shall be compensated for Services provided pursuant to Clause 3, 4 (Paragraph 2), 5, 6 (Paragraph 2) and 6 (Paragraph3) (e.g., surrendering the Data carriers, contacting the Data subjects, examinations).

4. Customers Obligations

The Customer shall inform the Provider immediately of any errors or irregularities with regard to Data protection regulations detected in the order results. All information shall be provided to support the case.

Clause 3 (paragraph 10) of this Annex shall apply accordingly, in case a claim should be raised by a Data subject against the Customer with regard to any claims under Article 82 of the GDPR.

The Provider should be informed by the Customer about the contact person of the Customer who is in charge of any Data protection issues arising within the scope of the Agreement. This shall be done especially in the case if the contact person differs from the contact person already named by the Customer.

5. Data Subject Requests

In case of requests to the Provider for correction, deletion, or information by a Data subject, the Provider shall refer the Data subject to the Customer provided that the assignment to the Customer is possible according to the information provided. The Provider shall immediately forward the request to the Customer. The Customer shall be supported by the Provider within the scope of its commercially reasonable possibilities and on instruction, to the extent agreed. The Provider shall not be liable if it is not addressed properly or in due time, or if the request of the Data subject is not addressed by the Customer.

6. Provide Evidence

The Provider shall provide appropriate documentation to demonstrate evidence of compliance with the obligations laid down in this Annex.

In case of an inspection requested by the Customer, which could be necessary in individual cases, they shall be carried out during normal business hours without impacting operations and the timing shall be agreed, taking into account reasonable lead time. It could be possible that an additional confidentiality agreement is needed and some preparation is needed to put in place additional technical and organizational measures to ensure confidentiality of other Customers Data. Should the Customer or its assigned auditor be in a competitive relationship with the Provider, the Provider shall have a right of objection against the auditor.

Clause 6 (Paragraph 2) shall apply accordingly, if an inspection should be carried out by a Data protection supervisory authority or another governing supervisory authority of the Customer.

The effort related to this inspection will by charged by the Provider to the Customer according to the time used for this inspection, including the preparation, and in accordance to the rates indicated in Annex 3 of the Master Service Agreement.

7. Additional Commissioned Processors / Subcontractors

The commissioning of subcontractors by the Provider is permissible as long as they meet the requirements hereof within the scope of the subcontract. An example of the subcontractor is a PCI DSS compliant payment service provider to store and process credit card transactions.

In general, the Provider is free in the choice of the subcontractors and the Customer agrees that the Provider may engage subcontractors. The Provider shall provide a list of current subcontractors on request of the Customer within 14 days of the date of request.

The Provider shall be responsible for transferring its obligations, especially its Data protection obligations from the Annex to the subcontractor if this is needed.

8. Provide Information Obligations

In case the Customer's Data should be at risk with the Provider through insolvency or composition proceedings, through seizure or attachment, or through other events or measures of third parties, the Provider shall inform the Customer immediately. In such case, the Provider shall inform all Responsible Persons in this context that the ownership of the Data and the sovereign rights to the Data lies exclusively with the Customer as a "Responsible Person" within the meaning of the GDPR. The information shall be done immediately.

9. Miscellaneous

The liability shall be governed by the Master Service Agreement.

In all other respects, the provisions of the Contract and the Master Service Agreement shall apply. In the event of any contradictions between the provisions of this document and the provisions of the Contract, this document shall take precedence. Should any part of this document be invalid, this shall not affect the validity of the Contract and the remaining provisions hereof. Annex A and Annex B shall be integral part hereof.

Annex A to the Commissioned Processing Agreement

Subject matter of the commission:

- Use of the Service my.WAGILE.pro as Software as a Service of the Provider and the related processing of the Customer's Data

Type and purpose of the intended Data processing:

- The Provider shall process the Data only according to the agreement made. Personal Data processed by the Customer shall be transferred to the Provider within the scope of the Master Service Agreement.

Type of personal Data:

The Customer defined the Data transmitted to the Service:

- Customer master Data (company name, name of the contact person, related email address, physical address)
- Personal master Data (name of the person, related company, email address, phone number)
- Contract Data (billing information, payment Data)
- Provider Data (Provider name, costs)
- History of Data

Categories of data subjects:

The Customer defined the data transmitted to the Service.

- Project master Data (start / end dates, scope statement, budget, project manager, sponsors)
- Project detailed Data (deliverables, milestones, decision, risks, dependencies, related resources, related Provider Data, related budget, related costs)

Deletion, blocking, and correction of Data:

Requests for changes, blocking, deletion shall be addressed to the Customer; otherwise the provisions of the Contract shall apply.

Annex B to the Commissioned Processing Agreement

The following organizational and technical measures are fundamental for Data processing

System access control:

- Logging of system access
- Secure transmission of authentication credentials in the network
- Easy authentication of employees (by username/password) with a high level of protection
- System access protection (authentication)
- Prohibition of saving function for passwords and/or form entries
- Blocking in case of unsuccessful attempts/inactivity, and process for resetting blocked access codes
- Administration and documentation of personal authentication media and access authorizations
- Definition of authorized persons
- Automatic and manual system access blocking

Data access control:

The following measures are available for Data access control:

- Logging of Data access
- Implementation of Data access restrictions
- Creation of an authorization concept
- Awarding of minimal authorizations
- Administration and documentation of personal Data access authorizations

Transport/transfer control:

The following measures are available for transfer control:

- Secure Data transmission between server and Customer, in the backend and to external systems
- Hardening of the back-end systems
- Implementation of security gateways at network transfer points
- Machine-to-machine authentication
- Description of all interfaces and the transmitted personal Data fields
- Process for collection and disposal
- Data carrier management (procedure)
- Privacy-oriented deletion/destruction procedure

Input control:

The following measures are available for input control:

- Logging of entries and Documentation of input authorizations

Commission control:

The following measures are available for input control:

- Logging of entries and Documentation of input authorizations

Availability control:

The following measures are available for availability control:

- Emergency plan
- Backup concept and Storage of backups
- Inspection of emergency infrastructure

Separation rule:

The following measures are available for intended use control:

- Efficient data collection
- Separate processing

----- END -----