DPA – Data Processing Agreement

Data Controller Appointment Agreement

Pursuant to Article 28 of the General Data Protection Regulation (GDPR), this agreement is concluded between the Supplier, as defined below, and the customer who has entered into contracts with the Supplier and accepts this agreement.

Provider:
DWMP S.r.l., with registered office in Modena (MO), Via Dei Falegnami 26, Tax Code and VAT Number 03306000369

1. Definitions and interpretation

(1) The preamble forms an integral part of this Agreement. In the Agreement, the following terms and expressions shall have the meanings associated with them below:

- **Personal Data**
  Has the meaning attributed by Data Protection Legislation and includes, by way of example, all data provided, stored, transmitted, received, or otherwise processed, or created by the Client or the End User in connection with the use of the Services, to the extent such data is processed by the Provider under the Contract.

- **Adequacy Decision**
  Means a decision of the European Commission, adopted pursuant to Article 45(3) of the GDPR, determining that the laws of a given country ensure an adequate level of protection for personal data, as required by Data Protection Legislation.

- **Notification email**
  Means the email address(es) provided by the Client at the time of subscribing to the Service or through any other official channel to the Provider, to which the Client wishes to receive notifications from the Provider.

- **Provider Personnel**
  Means the Provider's officers, employees, consultants, and other personnel, excluding the personnel of any Additional Data Processors.

- **Request**
  Means a request for access by a Data Subject, a request for deletion or rectification of Personal Data, or a request to exercise any other rights provided under the GDPR.

- **Additional Data Processor**
  Means any subcontractor to whom the Provider has subcontracted any of its contractual obligations and who, in performing such obligations, may collect, access, receive, store, or otherwise process Personal Data.

- **Service(s)**
  Means the service or services subject to the Contracts entered into from time to time between the Client and the Provider.

- **End User**
  Means any ultimate user of the Service, Data Controller.

- **Personal Data Security Breach**
  Means a security breach that accidentally or unlawfully results in the destruction, loss, alteration, unauthorized disclosure, or access to Personal Data, occurring on systems managed by the Provider or otherwise under the Provider's control.

2. Roles of the parties

(1) The Parties acknowledge and agree that the Provider acts as Data Processor in relation to Personal Data, and the Client generally acts as Data Controller of the Personal Data.

(2) Where the Client processes data on behalf of another Data Controller, the Client may act as Data Processor. In such case, the Client warrants that the instructions given and the actions taken in relation to the processing of Personal Data, including the Client's appointment of the Provider as an Additional Data Processor pursuant to this Agreement, have been authorized by the relevant Data Controller.

(3) The Client undertakes, upon simple written request, to provide the Provider with documentation evidencing the Data Controller's authorization for the processing activities and the appointment of the Provider as an Additional Data Processor.

(4) Each Party undertakes to comply, in the processing of Personal Data, with its respective obligations under the applicable Data Protection Legislation.

3. Subject matter, duration, personal data processed and categories of data subjects

(1) **Subject matter**

- This Agreement governs the appointment of the Data Processor and the provision of instructions thereto regarding the processing of Personal Data. The processing activities that the Processor may carry out are limited to those strictly necessary for the purpose of the main contract entered into by the Parties at the activation of the Service(s).

(2) **Duration**

- This Agreement shall be effective as of the Effective Date of the Agreement and shall automatically terminate upon the deletion of all Personal Data by the Provider.

(3) **Categories of personal data**

- For the purposes of providing the Services under the General Terms and Conditions, the Provider processes the following categories of Personal Data provided, stored, transmitted, or generated by the Client (including its authorized collaborators using the Services and the individuals for whom the Services are provided, or End Users) in connection with the use of the Product:

    1. identification and contact data**,** such as**:**
        - first name, last name
        - email, phone number
        - company affiliation
        - role/job position

2. information relating to the operation of the service.
3. commercial data, such as:
   - negotiation history
   - offers, orders, contracts
   - commercial preferences
   - notes and customer interactions
4. communication-related data**,** such as:
   - emails sent/received through the system
   - communication content
   - contact history
5. billing, accounting, and payment data, such as:
   - tax addresses
   - VAT number / tax identification number
   - billing data
   - payments received
6. access credentials and log data, such as:
   - username/email
   - access timestamps
   - IP addresses
   - operational logs
7. technical data relating to service usage, such as:
   - information on feature usage
   - errors and application logs

⚠️ **Exclusion of Payment Data**
The Supplier does not process or store payment card data (such as card numbers, CVV codes, authentication data, or other sensitive financial information). Any payments are managed exclusively by certified third-party providers (e.g., PayPal, Stripe), whose systems are used directly by the Client or the End User.

(4) **Categories of Data Subjects**

- In the provision of the Services, the Provider processes Personal Data provided, transmitted, stored, or created by the Client in the context of using the Service, relating to the following categories of data subjects:

  1. individual clients of the Clients
  2. contacts, employees, and collaborators of the Client's clients
  3. potential clients (leads/prospects)
  4. agents, representatives, and mandatary parties
  5. users authorized by the Client to use the service
  6. third parties whose data is processed by the Client within the scope of its activities (e.g., suppliers, partners, professional contacts)

(5) **Special Categories of Data (Art. 9 GDPR)**

- The system is not intended for the processing of data belonging to special categories.
  The Client undertakes not to enter:

  1. health data
  2. biometric data

3. data relating to political or religious opinions
4. other sensitive data

Should such data be entered, the Supplier:

1. is not responsible for it
2. may proceed with deletion where technically possible

(6) **Client Instructions**

- The Supplier processes data exclusively on the Client's documented instructions.
  The Supplier does not independently determine the categories of data entered by the Client into the system, limiting its role to processing data on behalf of the Client.
  The Client undertakes not to enter into the system data belonging to special categories under Art. 9 GDPR (e.g., health data, biometric data, data relating to political or religious opinions), unless otherwise agreed in writing between the Parties.
  The Client is responsible for:

  1. the lawfulness of the processing
  2. the accuracy of the data entered
  3. the management of legal bases

4. Processing within the EU and EEA

(1) The Processor undertakes not to transfer any Personal Data abroad (i.e., outside the territory of the EEA) without the prior written authorization of the Controller and in accordance with the Controller's documented and specific instructions.

(2) The parties mutually acknowledge that the processing of personal data under this agreement shall not take place outside the EEA.

5. Technical and organizational measures

(1) Prior to executing this appointment, the Processor shall implement all appropriate technical and organizational measures for the protection of Personal Data and shall provide the Controller with a document detailing all security measures adopted by the Processor, including specific reference to the execution of this Agreement. Such measures are subject to the Controller's review and prior approval. Once approved by the Controller, these measures, as documented in the aforementioned document, shall become an integral and substantial part of this Data Processing Agreement and shall be deemed fully incorporated herein. Should the Controller, through inspection or audit, determine that modifications are necessary, such modifications shall be made in agreement between the Parties.

(2) The Processor guarantees the security of processing pursuant to Articles 28(3)(c) and 32 of the GDPR, in particular in accordance with Article 5(1) and (2) of the GDPR. These measures must ensure the security of the data and a level of protection appropriate to the risk to the confidentiality, integrity, availability, and resilience of systems. Pursuant to Article 32(1) GDPR, in assessing the adequacy of security measures, account shall be taken of the state of the art, implementation costs, the nature, scope, context, and purposes of processing, as well as the likelihood of a personal data breach and the severity of the potential risks to the rights and freedoms of natural persons.

(3) Technical and organizational measures are subject to evolution and technological progress. Therefore, the Processor may adopt appropriate alternative measures suitable to the changing technological context.

In such cases, the level of security of processing must not be reduced. Any substantial modification must be documented.

6. Data subject rights

(1) The Processor undertakes to cooperate with the Controller and to provide the fullest possible assistance, to the extent reasonably practicable, in order to facilitate the Controller in responding to requests from Data Subjects for the exercise of their rights.

(2) In particular, the Processor undertakes to (i) promptly notify the Controller of any request received from Data Subjects regarding the exercise of their rights and, where feasible or appropriate, to (ii) assist the Controller in designing and implementing all technical and organizational measures necessary to respond to such requests.

(3) Without prejudice to the fact that the responsibility for responding to and fulfilling Data Subject requests rests solely with the Controller, the Processor may be instructed to process certain specific requests, provided that this does not require disproportionate effort and is carried out under the Controller's specific written instructions.

7. Additional obligations of the Processor

In addition to the provisions of this Agreement, the Processor shall comply with all legal requirements set forth in Articles 28–33 of the GDPR. To this end, the Processor guarantees the following:

- **Appointment of a Data Protection Officer (DPO)**
  Mr. Alessandro Dina, reachable at the following number: +39 059-2270431 or at the email address: dina@dwmp.it, shall act as the point of contact on behalf of the Processor.

- **Confidentiality**
  The processing activities governed by this appointment agreement shall be carried out solely by employees, collaborators, or agents who have been previously instructed by the Processor regarding the proper handling of Personal Data and who are contractually bound by confidentiality obligations pursuant to Articles 28(3)(b) and 32 GDPR. The Processor, as well as anyone acting under its authority with access to Personal Data, shall not process such data unless instructed to do so by the Controller, including via this appointment, except where expressly required by law.

- **Technical and organizational measures**
  The Processor shall implement and maintain appropriate technical and organizational measures in the context of this appointment agreement, as specified under Article 32 GDPR. The Processor shall periodically review internal processes and technical and organizational measures to ensure that processing within its area of responsibility complies with the requirements of data protection legislation and the rights of Data Subjects. The Processor shall ensure that the Controller can verify the technical and organizational measures within the scope of its monitoring rights as set out in Section 9 of this Agreement.

- **Cooperation with supervisory authorities**
  The Controller and the Processor shall cooperate, upon request, with the competent supervisory authority. The Controller shall be promptly informed of any inspections or actions carried out by the supervisory authority insofar as they relate to activities conducted under this Agreement. This obligation also applies where the Processor is subject to or involved in an investigation by a competent authority regarding any breach of data protection provisions in the course of activities under this Agreement. To the extent that the Controller is subject to inspection by a supervisory

authority, administrative fines, precautionary measures, criminal proceedings, claims from Data Subjects or third parties, or any other legal action in connection with the processing of data by the Processor under this appointment, the Processor shall make all reasonable efforts to support the Controller.

8. Sub-Processors

1) The Controller hereby authorizes the Processor to engage third-party Data Processors. Such sub-processors, as required by law, shall be subject to the same contractual obligations contained in this Agreement pursuant to Article 28(4) GDPR.

(2) As of the date of execution of this Agreement, the Parties mutually acknowledge that the Processor uses the following sub-processors, with whom it undertakes to enter into contractual agreements compliant with the provisions of Article 28(4) GDPR:

	A	B	C
1	**Sub-processor (company)**	**Address / Country**	**Delegated processing activities**
2			
3			

(3) It is understood that the disclosure of data to a third-party Data Processor may only occur once all the conditions for the appointment referred to in paragraph (1) of this section have been met.

(4) The Processor shall maintain an up-to-date list of sub-processors. Any changes to such list must be communicated to the Controller without undue delay, granting the Controller the right to object. In the event of an objection, the Processor shall have the right to terminate the Agreement with the Controller without notice.

(5) The Processor shall be fully liable for the acts and omissions of its sub-processors towards the Controller.

(6) Should a sub-processor perform its activities outside the EU/EEA, the Processor shall ensure the lawfulness of the data transfer outside the EEA, as described in Section 4 of this Agreement.

9. Controller's audit rights

(1) The Controller shall have the right to carry out audits or to have them carried out by an auditor appointed from time to time. The auditor shall assess the Processor's compliance with this Data Processing Agreement during its business operations through spot checks, which shall generally be notified in advance.

(2) The Processor shall allow the Controller to verify compliance with its obligations under Article 28 GDPR. Upon request, the Processor shall provide the Controller with all necessary information, including, in particular, evidence of the implementation of technical and organizational measures.

(3) Evidence of the implementation of such measures, which may also relate to activities beyond the scope of this Agreement, may be provided by means of:

- compliance with codes of conduct approved pursuant to Article 40 GDPR;
- certifications issued under a certification mechanism approved pursuant to Article 42 GDPR;
- current certifications from auditors, reports, or excerpts of reports prepared by independent bodies (e.g., auditors, Data Protection Officers, IT security departments, data protection auditors);

- appropriate certifications issued by IT security or data protection auditors.

(4) The Processor may charge the Controller a reasonable fee for carrying out the audits.

10. Assistance to the Controller

(1) The Processor shall assist the Controller in fulfilling its obligations regarding the security of Personal Data, the reporting of data breaches, data protection impact assessments, and prior consultations pursuant to Articles 32 to 36 GDPR, including, inter alia:

- ensuring appropriate protection standards through technical and organizational measures, taking into account the nature, circumstances, and purposes of the processing, the likelihood of data breaches, and the severity of the risk to natural persons that may result
- ensuring the immediate detection of breaches
- promptly reporting to the Controller any data breaches
- assisting the Controller in responding to Data Subject requests for the exercise of their rights

(2) The Processor may request from the Controller a reasonable fee for assistance services that are not included in the description of the Services and are not required due to errors, breaches, or conduct attributable to the Processor.

11. Controller's instruction rights

(1) The Processor shall not process any Personal Data under this appointment except on the Controller's documented instructions, unless required to do so by European Union law or the law of Member States.

(2) If the Controller requests a change in the processing of Personal Data pursuant to the documented instructions referred to in Section 3, the Processor shall immediately inform the Controller if it believes that such a change may result in a breach of data protection provisions. The Processor may refrain from carrying out any activity that could give rise to such a breach.

12. Liability

(1) The Supplier does not determine the categories of data entered into the system.

(2) The Client is responsible for the data uploaded and for its content.

(3) Each Party to this Agreement undertakes to indemnify the other Party for any damages or expenses arising from its own negligent breach of this Agreement, including any negligent breach committed by its legal representatives, subcontractors, employees, or other agents. Furthermore, each Party undertakes to hold the other Party harmless from any claims made by third parties arising out of or in connection with any negligent breach committed by the other Party.

(4) Nothing in this Agreement affects the provisions of Article. 82 GDPR.

13. Deletion and return of personal data

(1) The Processor shall not create copies or duplicates of the data without the Controller's knowledge and consent, except for backup copies to the extent necessary to ensure correct data processing, as well as for data whose retention is required by law.

(2) Upon termination of the provision of Services, for any reason, the Processor shall delete in a manner compliant with data protection or return to the Controller all Personal Data collected and processed under this appointment, unless applicable law requires further retention of the Personal Data.

(3) In any case, the Processor may retain all information necessary to demonstrate the proper and compliant execution of the processing activities even after the termination of the Agreement.

(4) The documentation referred to in paragraph (3) must, in any event, be retained by the Processor in compliance with statutory retention periods or as otherwise established. The Processor may deliver such documentation to the Controller at the end of the term of the Agreement to be released from the contractual retention obligation.

Annex 1

Technical and organizational measures

The Data Processor implements the following organizational security measures

CLOUD SaaS

1. Organizational security measures

a. User Policies and Disciplinary Rules
The Provider adopts detailed policies and disciplinary rules that all users with access to the information systems are required to comply with. These policies are intended to ensure behavior that respects the principles of confidentiality, availability, and integrity of data when using IT resources.

b. Logical access authorization
The Provider defines access profiles in accordance with the principle of least privilege, necessary for the performance of assigned tasks. Authorization profiles are identified and configured prior to the start of processing, in order to restrict access to only the data necessary for carrying out processing activities. These profiles are subject to periodic checks to verify that the conditions for their retention continue to apply.

c. Management of support interventions
Support interventions are regulated to ensure that only contractually agreed activities are performed and to prevent excessive processing of Personal Data, the ownership of which belongs to the Client or the End User.

2. Technical security measures

a. Communication line security
Within the scope of its responsibilities, the Provider adopts secure communication protocols in compliance with the best available technologies.

b. Authentication credentials
Systems are configured to allow access exclusively to individuals with authentication credentials, enabling their unique identification. Passwords are known only to the user and are stored encrypted using a one-way encryption algorithm, with the addition of a pepper (a secret value added to all passwords, stored separately, which further enhances protection against potential cyberattacks) and a salt (a unique random value for each user, ensuring that each password is

different even if two users choose the same keyword). Two-factor authentication (2FA) may also be used to further enhance security.

c. Brute-force protection
The login page is protected by Google reCAPTCHA, a service provided by Google that analyzes user behavior on the login page to distinguish between legitimate users and automated programs. This ensures that only real users can attempt to access the system.

d. Malware protection
Systems are protected against intrusions and malicious software through the use of appropriate electronic tools, which are updated periodically. Antivirus tools are employed and kept continuously up to date.

e. Logging
Systems are configured to allow tracking of access and, where appropriate, activities performed by different types of users (Administrator, Supervisor, User, etc.). These logs are protected by adequate security measures to ensure their integrity. Logs will be retained for a period of 12 months.

f. Backup & Recovery
Appropriate measures are adopted to ensure the restoration of data access in the event of data or electronic equipment damage, within defined timelines compatible with the rights of Data Subjects.

g. Data Center
Remote access is only possible from the IP address of DWMP's headquarters. Physical access to the Data Center may be performed exclusively by the provider. For details regarding the security measures adopted in relation to Data Center services provided by Additional Data Processors, reference is made to the security measures described by such Additional Data Processors and made available on their official websites at the following addresses (or at those subsequently made available by the Additional Data Processors):

For Data Center services provided by Amazon Web Services:
https://aws.amazon.com/it/compliance/data-center/controls/
https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and-compliance/welcome.html
https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
https://d1.awsstatic.com/Supplementary_Addendum_to_the_AWS_GDPR_DPA.pdf

For Data Center services provided by Contabo:
https://contabo.com/en/legal/privacy/

For Data Center services provided by Aruba Cloud:
https://www.aruba.it/gdpr-regolamento-europeo-privacy.aspx
https://www.cloud.it/sicurezza.aspx