

Data Processing Agreement

Data Controllers

Reference: GDPR-DOC-APDRT

Version: 2.1

Date: 16/07/2026

Classification: Available to Signatories and Supervisory Authorities

GDPR - Organisational Measures

1. Contracting Parties and Points of Contact

1.1. Data Controller: Entity or taxable person acting in a professional capacity processing data in accordance with instructions provided by the Data Processor during negotiations and/or acquisition proposal. For the purposes of this Data Protection Agreement (DPA), the Subsequent Data Processor [Sub-processor] is:

- XXXXXXXX
XXXXXXX
XXXXXXX
XXXXXXX

The point of contact for all matters relating to personal data protection, this agreement, and potential personal data breaches is:

- Job title
email | telephone

1.2. Data Processor: Entity processing data required for the invoicing process on behalf of the data controller. For the purposes of this DPA, the Data Processor is:

- Moloni, Unipessoal Lda
Av. José Malhoa, n.º 2 - Tardoz, Edifício Malhoa Plaza, escritório 1.5
1070-325 Lisboa
VAT number 513 321 527;

The point of contact for all matters relating to personal data protection, this agreement, and potential personal data breaches is:

- Data Protection Officer
dpo@moloni.pt | 211450112

2. Introduction

2.1. Both Parties confirm that the signatories have sufficient powers to enter into this DPA. This Agreement shall form part of and govern the processing of personal data linked to the main service contract established between the Parties, whose main object is:

- Issuance of tax-relevant documents and underlying operations supporting and organising information.

2.2. The Data Processor undertakes to contribute to the Data Controller's privacy framework in a reasonable manner and under the terms of this document to enable the Data Controller to be transparent with its own customers, in accordance with applicable privacy legislation requirements. As part of this, the Data Processor confirms that i) it is aware of a Data Processor's obligations under the GDPR, ii) how this affects the conduct of its own business, and iii) that it shall incorporate compliance with the General Data Protection Regulation (GDPR) into the performance and delivery of the service it provides, under the terms of this document, paying particular attention to the provisions of Articles 25, 28, 30, and 32 to 36 of the General Data Protection Regulation.

3. Scope of Application

3.1. This agreement governs data processing carried out by the Data Processor upon subscription by the Data Controller (Moloni Client) and highlights how the Data Processor shall ensure data privacy through the adoption and implementation of technical and organisational measures that demonstrate compliance with applicable regulations, in particular the GDPR.

3.2. Data processing carried out by the Data Processor serves the sole purpose of delivering the service contributing to the main object referred to in Clause 2.1. The Data Processor undertakes not to process data covered by this contract for any purpose outside the scope of the service to be delivered.

3.3. The parties also agree that this document takes precedence over other provisions established under other service agreements or data protection agreements previously existing between the parties. This agreement shall remain valid as long as the main service object contract remains in effect.

4. Obligations and Rights of the Data Controller

4.1. The Data Controller has legal authority to process and disclose to the Data Processor and, where applicable, to additional sub-processors as may prove necessary, all Personal Data required for the intended processing.

4.2 The Data Controller is also responsible for controlling the accuracy, integrity, content, reliability, and lawfulness of the Personal Data disclosed to the Data Processor.

4.3. The Data Controller further assumes the duties of providing information to Data Subjects and authorities regarding the processing of Personal Data in accordance with mandatory data protection legislation.

4.4 When using the services provided by the Data Processor under the Service Agreement, the Data Controller shall not disclose any Sensitive Personal Data to the Data Processor, unless explicitly agreed in Annex I to this agreement.

5. Obligations of the Data Processor

5.1. The Data Processor shall only process personal data on behalf of and in accordance with the instructions of the Data Controller, as set out in writing in the Terms of Use and in this agreement. From these documents, it can be inferred that data processing shall be carried out within the limits of the Law and other applicable regulations, to fulfill all obligations arising from the Terms of Use subscribed to at the start of the commercial relationship, as stipulated by the rules and principles of operation for regular use of the processor's service and also in accordance with the specifications of this agreement. For all due purposes, subscription to, activation of, or regular use of the Service—which may include, by default or natively, features based on Artificial Intelligence, virtual assistants, intelligent agents, audio transcription, or automated document reading (pursuant to Clause 7 of the Terms of Use), as well as voluntary interaction with technical support and commercial assistance channels using equivalent technologies (pursuant to Clause 19 of the Terms of Use)—constitutes authorisation from the Data Controller for the Data Processor to transit and process the necessary data with external AI technology partners.

5.2. Should the Data Processor have or become aware that data processing activities infringe the GDPR or other applicable privacy legislation, it shall notify the Data Controller of such potential data privacy breaches.

5.3. The categories of Data Subjects and Personal Data subject to processing linked to this agreement are described in Annex 1 to this agreement.

5.4. The Data Processor shall guarantee the confidentiality, integrity, and availability of Personal Data in accordance with the standards and requirements provided for in Article 32 of the GDPR and other applicable privacy legislation. The Data Processor shall conduct its business in accordance with systemic, organisational, and technical measures adopted to ensure an appropriate level of security, taking into account the state of the art and implementation costs relative to the risk represented by the processing activities.

5.5. The Data Processor shall assist the Data Controller in implementing security measures through appropriate technical and organisational measures in fulfilling its obligations and, indirectly, in fulfilling the obligations of the Data Controller (Moloni Clients), under applicable privacy legislation. Such assistance is particularly relevant in the event of requests to exercise rights by data subjects concerning privacy rights under Chapter III of the Regulation, or in other privacy compliance matters under the GDPR, particularly regarding the requirements described in Articles 32 to 36 of the GDPR.

5.6. If the Data Controller requires additional information or assistance regarding security measures, documentation, or other forms of information on how the Data Processor processes Personal Data, and such requests exceed standard information provided by the Data Processor to comply with applicable privacy legislation, it shall formulate a specific request that will be analysed on a case-by-case basis, taking into account requested data categories and implications these may have on the company's proprietary processes. Processing such requests for supplementary information may be subject, upon prior notice, to a processing fee calculated based on the allocated resources.

5.7. The Data Processor and its team shall guarantee confidentiality regarding Personal Data subject to Processing under the Agreement. This provision shall also apply after termination of the Agreement by the Data Controller and to workers serving Moloni, regardless of length of service and employment relationship established.

5.8. By notifying the Data Controller without undue delay, the Data Processor shall enable the Data Controller to comply with legal requirements regarding notification to data authorities or Data Subjects about data privacy incidents that may occur.

Additionally, to the extent appropriate and lawful, the Data Processor shall notify the Data Controller with:

- i) Early Warning: Within a maximum period of 24 hours after becoming aware of the incident, indicating whether it may originate from unlawful actions or presents a risk of propagation;
- ii) Incident Notification: Within a maximum period of 72 hours after becoming aware, accompanied by a detailed report with the initial severity assessment.

5.9. The Data Processor shall not respond directly to requests from personal data subjects, unless authorized to do so by the Data Controller. The Data Processor shall not disclose Personal Data transmitted to it, except if required by law, such as through a court order or similar warrant whose justification is deemed valid.

5.10. The Data Processor does not assume the risk inherent in the Data Controller's use of third-party integrations intended to automate processes via the API made available by the Data Processor. The reliability of this type of integration is only ensured in the case of proprietary solutions.

5.11. The Data Processor may process Personal Data of users and regarding service usage by Data Controllers, based on the Data Processor's legitimate interest in the continuous improvement of the platform's user experience and security (pursuant to point (f) of Article 6(1) of the GDPR), when necessary to obtain feedback and improve the service. The Data Controller grants the Data Processor the right to use and analyze activity data associated with their use of the Service for product optimization and improvements or as a means to improve service delivery, as well as to allow the Data Processor to create new features and functionality for subsequent incorporation into the product and/or new versions. It is expressly clarified that this right encompasses analyzing usage metrics and cross-referencing subscription and commercial management (CRM) data for churn prevention, plan optimization suggestions (upsell), or direct marketing communications from the platform itself, with the user guaranteed the right to object (opt-out) in account settings. Whenever such processing involves non-aggregated personal data, the Data Processor undertakes to apply strict pseudonymisation measures, ensuring that data cannot be attributed to a specific data subject without the use of additional information kept separately. In this context, Moloni shall be considered Data Controller, falling outside the scope of this agreement.

5.12. By using the service, the Data Controller will add data to the Software and acknowledges that the Data Processor may use said Customer Data in structured, pseudonymised, or non-aggregated formats, for purposes of improving services provided to customers, research, training, educational and/or statistical purposes, provided that technical guarantees of identity isolation provided for in clause 5.11 are ensured.

6. Use of Subsequent Processors [Sub-processors]

6.1. As part of providing services to the Data Controller and in accordance with Service Agreements as well as this agreement, the Data Processor shall make use of sub-processors and the Data Controller gives its general consent to the use of sub-processors selected and/or to be selected by the Data Processor. These sub-processors may be companies within the Visma group, to which Moloni also belongs, or external third-party sub-processors. All sub-processors

are included in Annex B. The Data Processor shall ensure that sub-processors agree to assume responsibilities corresponding to the obligations established in this agreement and in the Terms of Service. General consent to the use of sub-processors explicitly encompasses providers of Artificial Intelligence computing and infrastructure services required for the execution of intelligent tools provided natively by the platform.

6.2. Should sub-processors be located outside the EU or EEA, the Data Controller grants the Data Processor authorization to analyze appropriate legal bases for transferring Personal Data outside the EU/EEA on behalf of the Controller, under the terms of this document, by consulting Adequacy Decisions and adopting EU Standard Contractual Clauses.

6.3. If the Data Controller objects to a new sub-processor within 30 days of its engagement being made public, the Data Processor and Data Controller shall review documentation of the sub-processor's compliance efforts to ensure compliance with applicable privacy legislation. If the Data Controller still objects and has reasonable grounds to do so, the Data Controller cannot withhold consent against the use of such sub-processor (due to the specific nature of online standard Software and mass subscription distribution model under terms of service), but the Data Controller may terminate the Service Contract for which the disputed sub-processor is being used. If it is not possible to isolate the process in which sub-processors are being used, total termination of the Moloni supply contract shall be considered.

7. Security

7.1. The Data Processor is committed to delivering a high level of security across its products and services, achieved through organizational, technical, and physical security measures in accordance with information security measure requirements described in Article 32 of the GDPR.

7.2. The Service Agreement establishes data security measures or procedures implemented by the Data Processor in processing Personal Data under its care. The Data Controller shall be responsible for appropriate and adequate security of equipment and IT environment under its responsibility.

8. Audit Rights

8.1 The Data Controller may audit the Data Processor's compliance with this agreement up to once a year. If required by legislation applicable to the Data Controller, it may request audits with shorter periodicity than announced. To request an audit, the Data Controller must send the Data Processor a detailed audit plan at least four weeks prior to the proposed audit date, describing proposed scope, duration, and start date. If a third party conducts the audit, it shall, as a general

rule, be mutually agreed between Data Controller and Data Processor. However, if the environment where processing is conducted is multi-vendor, the Data Controller grants the Data Processor authority to decide, for security reasons, that audits will be conducted by a neutral external auditor of its choice.

8.2. If the audit scope requested by the Data Controller is covered in an ISO standard report or similar conducted by a qualified external auditor in the last twelve months, and the Data Processor confirms no material changes are known in audited measures, the Data Controller agrees to accept those conclusions instead of requesting a new audit of measures covered by the report.

8.3 In any event, audits shall be conducted during normal business hours at the processor's premises or others under its responsibility, in a format subject to processor regulations and policies, and may not unreasonably interfere with its business activities.

8.4 The Data Controller shall be responsible for any costs arising from audits it requests. Furthermore, assistance requests to the Data Processor may be subject to fees, analyzed on a case-by-case basis.

9. Term and Termination

9.1. This agreement is valid as long as the Data Processor processes personal data on behalf of the Data Controller and takes effect immediately upon acceptance of Terms of Service or, if necessary, with specificities agreed in Annex A.

9.2. Conversely, this agreement terminates automatically upon termination of the Service Agreement provided for in respective terms. Upon termination of this agreement, the Data Processor shall delete or return Personal Data processed on behalf of the Data Controller, in accordance with applicable clauses in Terms of Use and Data Retention Policy referenced therein. Such deletion shall occur as soon as reasonably possible, unless local or EU legislation requires additional storage.

10. Amendments

10.1. Amendments to this agreement become valid upon publication. In the case of agreements with specificities under clause 9.1, amendments shall only take effect upon signing a new agreement.

10.2. Should any provision of this agreement become void, this shall not affect remaining provisions. The Parties shall replace the void provision with a legal provision reflecting the same purpose.

11. Liability, Applicable Law, and Jurisdiction

11.1. For the avoidance of doubt, Parties agree and acknowledge that each Party shall be liable and responsible for paying administrative fines and damages directly to data subjects that the Party was required to pay by authorized data protection authorities or courts, in accordance with applicable privacy legislation. Liability matters between Parties shall be governed by liability clauses in Terms of Service agreed upon subscription and provision of the Moloni platform.

11.2. Applicable jurisdictions in dispute resolution are also referred to in the Terms of Use.

For Moloni Unipessoal – Data Processor

Signature

Name

Position

Date

For XXXXXX – Data Controller

Signature

Name

Position

Date

Annex A – Data Subjects, Types of Personal Data, Purposes, Description, and Duration of Processing

A.1. Categories of Personal Data Subjects

- End customers of the Moloni ON user
- Employees of the Moloni ON user
- Contact persons of the Moloni ON user

A.2. Categories of Processed Personal Data

- Billing information such as name, address, tax identification number, etc.
- Information regarding professional ties and positions held
- Current account information, obtained through simple summation and without profiling end customers
- Voice data and audio recordings (exclusively within the scope of voice commands for virtual assistants or interactions with technical support and commercial assistance channels)

Note: Special categories of personal data within the meaning of Article 9 of the GDPR are not processed.

A.3. Processing Purposes

The processing purposes for which Moloni ON processes personal data on behalf of clients are:

- Delivery of the invoicing service in accordance with the subscribed Terms of Use;
- Conducting technical and commercial assistance operations (including potential use of virtual customer service assistants, automated message analysis, or communication transcription via Artificial Intelligence systems, pursuant to Clause 19 of the Terms of Use);
- Management of the commercial relationship with clients and official agents.

A.4. Description of Processing

Data processing carried out by Moloni derives from the Terms of Use and primarily comprises personal data being recorded, stored, edited, placed on tax, supporting, and internal management documents, and reported to clients themselves and supervisory control authorities.

A.5. Duration of Processing

Given the specific nature of processing related to personal data underlying tax documentation, the duration of processing is governed by the Data Retention Policy referenced in the Terms of Use.

Annex B – Sub-processor Overview

In order to safeguard trade secrets, physical infrastructure security, and the integrity of Moloni's technological ecosystem, the detailed and updated list of active sub-processors and respective data processing locations shall be made available confidentially and exclusively to signatories of this Agreement, upon a reasoned request addressed to the Data Protection Officer via email: dpo@moloni.pt.

Within the framework of Regulation (EU) 2024/1689 (AI Act), the Data Processor undertakes not to use personal data or voice recordings processed on behalf of the Data Controller for training or developing proprietary Artificial Intelligence models. Furthermore, contracts entered into with third-party providers of AI infrastructure and language models (LLMs) (as provided for in Clause 7 of the Terms of Use) prohibit contracted partners from making the same use for service delivery.