DATA PROCESSING AGREEMENT

This Data Processing Agreement (hereinafter, the "**DPA**") is applicable to the users who have accepted the Terms and Conditions and Privacy Policy of Maisa Inc, with its registered office in the state of Delaware, with offices at 1111B S Governors Ave STE 3624 Dover, DE 19904 (hereinafter, "**Maisa**") and regulates the processing of any personal data of the Maisa users, as a Data Controller, (each a "**User**") by Maisa, as a Data Processor.

With respect to provisions regarding processing of personal data, in the event of a conflict between the Terms and Conditions or Privacy Policy and this DPA, the provisions of this DPA shall prevail.

CLAUSES

1. Definitions

Capitalized terms in this DPA shall have the same meaning as in the General Data Protection Regulation 679/2016 ("**GDPR**" or "**Data Protection Regulations**").

2. Object and Term

This DPA regulates the processing of Personal Data by Maisa in relation to the provision of the services regulated in the Terms and Conditions and accepted by the User (hereinafter, the "**Services**"). Such Personal Data shall be under the responsibility of the User and/or its customers.

The term of the processing will be for the duration of the provision of the Services by Maisa to the User, in this case, Maisa shall destroy or return to the User all Personal Data and any copy of it, as well as any support or other document containing any Personal Data

3. Data accessed and purpose of the processing

Maisa may have access to the type of Personal Data and the categories of Data Subjects described below in Appendix I. Maisa may also have access to such personal data only for the purposes described in Appendix I.

Maisa will process the Personal Data in accordance with the Standard Contractual Clauses set out in Annex I.

4. Obligations of Maisa

As established in the GDPR, Maisa shall:

a) Process Personal Data only on the basis of documented instructions from the User, including transfers of Personal Data to a third country or international organization, unless otherwise required to do so under Union law or applicable Member State law.
b) Ensure that all the persons authorized to process Personal Data have undertaken to respect confidentiality or are subject to an obligation of confidentiality.
c) Take all appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing, in particular by:
    i. The pseudonymisation and encryption of Personal Data;

ii. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
iii. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
iv. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

d) Not to subcontract another data processor, with the exceptions described in clauses 7 and 8.
e) Assist the User, taking into account the nature of the processing, through appropriate technical and organisational measures, whenever possible, so that it can comply with its obligation to respond to requests for the exercise of the rights of the data subjects.
f) Assist the User in ensuring that it complies with their obligations, taking into account the nature of the processing and the information that is available to Maisa.
g) At the User's option, destroy or return all Personal Data once the processing services have been completed and destroy any existing copies unless the retention of such Personal Data is required under Union or applicable Member State law.
h) Make available to the User all information necessary to demonstrate compliance with the obligations set out in this Article, as well as to allow and contribute to the performance of audits, including inspections, by the User or another auditor authorized by the User.
i) Process the Personal Data of the User in a way that ensures that the personnel in charge, if any, follow the instructions of the User.
j) Ensure that the Data Protection Officer or, in his or her absence, the Privacy Officer is involved in a timely and appropriate manner in all matters relating to the protection of Personal Data of the User.
k) Adhere to the Code of Conduct that may be approved by the corresponding Commission or body, if applicable.
l) Keep a record of processing activities in the event of processing personal data that involve a risk to the rights and freedoms of the data subject and/or on a non-occasional basis, or that involves the processing of special categories of data and/or data relating to convictions and offences.

5. Exercise of Data Subjects rights

During the Processing of Personal Data, the Data Subject may apply for the exercise of the rights of access, rectification, erasure, restriction, object and data portability. Once the request has been submitted, the User shall provide a response to the Data Subject within a period of one month, which may be extended by two further months where necessary, taking into account the complexity and number of the requests. The response to the request shall be in the same format as that used by the Data Subject, unless otherwise requested.

When the Data Subject exercises its rights to the User, Maisa shall cooperate with the User in order to satisfy the exercise of the Data Subject's rights requested, in particular, Maisa shall provide the User with all information necessary for the fulfillment of the Data Subject's requests.

Furthermore, in the event that the Data Subject exercises its rights to Maisa, Maisa shall inform the User about such request without delay and at least within 5 working days from its receipt. Maisa shall also inform the Data Subject of the possibility of exercising such rights to the User.

6. Subcontracting

Except as set out in Appendix II, Maisa may not under any circumstances subcontract its services to another Sub-processor. In the event that such subcontracting is necessary, Maisa must have the written authorization of the User, and the Sub-Processor must state the purpose and objectives of the subcontracting as well as the identification of the Sub-Processor.

7. International Transfers

Maisa may not make any international transfer of the Personal Data of the User without the User's express authorization, with the exception of transfers to the international subcontractors mentioned in Appendix II, provided that an agreement with appropriate contractual guarantees is signed with each of them, as prescribed by the Data Protection Regulations.

In particular, Maisa will process personal data within an EU Member State through the Sub-processors listed in Appendix II. In the event that the Sub-processors carry out international transfers, Maisa will ensure that they comply with the appropriate safeguards under the Data Protection Regulations.

8. Security breach

In accordance with the Data Protection Regulations, in the event of a Personal Data breach of the User, Maisa shall notify the User of such breach without undue delay, and if possible, no later than 24 hours after it happened.

9. Obligations of User

User represents, warrants, and covenants that: (i) it has (and will have) processed, collected, and disclosed all Personal Data in compliance with applicable law and provided any notice and obtained all consents and rights required by applicable law to enable Maisa to lawfully process Personal Data as permitted by the Terms and Conditions and/or this DPA; (ii) it has (and will continue to have) full right and authority to make Personal Data available to Maisa under the Terms and Conditions and this DPA; and (iii) Maisa's processing of Personal Data in accordance with the Terms and Conditions, this DPA, and/or User's instructions does and will not infringe upon or violate any applicable law or any rights of any third party. User shall indemnify, defend, and hold Maisa harmless against any claims, actions, proceedings, expenses, damages, and liabilities (including without limitation any governmental investigations, complaints, and actions) and reasonable attorneys' fees arising out of Customer's violation of this Section 9. Notwithstanding anything to the contrary in the Terms and Conditions, User's indemnification obligations under this Section 9 shall not be subject to any limitations of liability set forth in the Terms and Conditions.

Appendix I

In accordance with the provisions set out herein and in the GDPR, Maisa may access and process the type and category of Personal Data provided by the User set out hereunder (Personal Data):

Data Subjects	Data Categories	Purposes
Identifiable Person	*Personal data included by the Users in the Platform which may be included in any prompt*	*Providing the Services to the* User

The provision of the contracted Services implies the performance by Maisa of the following processing: access, collection, registration, organization, storage, suppression and destruction, usage.

Appendix II

Sub-processors	Type of processing	Location	International transfer	Privacy policy URL / SCC (if applicable)
AWS	Infrastructure Services	USA	Yes	https://aws.amazon.com/privacy/?nc1=h_ls
OpenAI	Artificial Intelligence services	USA	Yes	https://openai.com/es-ES/policies/eu-privacy-policy/
Antrophic	Artificial Intelligence services	USA	Yes	https://www.anthropic.com/legal/privacy
LlamaIndex	Document parsing	USA	Yes	https://www.llamaindex.ai/files/privacy-notice.pdf
Maisa AI Capital SL	Platform management and software services	Spain	No	(member of the Maisa AI Inc group)

ANNEX I. STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter,

delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses,

at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract

involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal.

When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred

personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Spain

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Spain.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Users of Maisa (Data Controller)

Activities relevant to the data transferred under these Clauses:

To include personal data in the prompts entered in the Platform.

Data importer(s): Maisa, Inc (Data Processor).

Address:

State of Delaware, with offices at 8 The Green STE R, Dover, County of Kent, Delaware, 19901

Activities relevant to the data transferred under these Clauses:

Process the personal data included by Users on the Platform.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The users of the User

Categories of personal data transferred

The personal data included by Users in the prompts.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Only when the User includes the Personal Data in the platform.

Nature of the processing

Access, collection, registration, organization, storage, suppression and destruction, usage.

Purpose(s) of the data transfer and further processing

To provide the services with the Users

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

During the term in which the User has the account in active status.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Hosting of the platform and the data

C. COMPETENT SUPERVISORY AUTHORITY

Agencia Española de Protección de Datos

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Hereinafter, Data the Processor shall have the right and the obligation to make decisions on the technical and organizational security measures to be implemented in order to create the necessary (and agreed) level of data security.

However, the Data Processor shall, in any case and as a minimum, implement the following measures agreed with the Controller:

1. **Physical Access Controls.**

Data Processor will take reasonable measures to prevent physical access, such as security personnel and secured buildings, to prevent unauthorized persons from gaining access to personal data.

2. **System Access Controls.**

Data Processor will take reasonable measures to prevent personal data from being accessed and/or used without authorization. These controls shall vary based on the nature of the processing and will include at minimum authentication via password and/or two-factor authentication, documented authorization processes, documented change management processes, and logging of access of the data.

3. **Data Access Controls.**

Data Processor will take reasonable measures to ensure that personal data is only accessible and manageable by properly authorized staff, direct database query access is restricted, and access rights to and within data processing systems are established and enforced to ensure that only authorized persons can access the data processing systems and the data within that they have the authorization to access. Moreover, these controls will be established and enforced to ensure that personal data cannot be read, copied, modified, or removed without authorization in the course of processing.
In addition to Sections 1-3, Data Processor warrant it has an implemented access policy which requires that access to its system environment, to personal data, and to other data are limited to authorized personnel only.

4. **Transmission Controls.**

Data Processor will take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of personal data by means of data transmission facilities is envisaged so personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport. Without limiting the foregoing, Data Processor shall ensure personal data is encrypted (at least 256 bit encryption) in transit and storage.

5. **Input Controls.**

Data Processor will take reasonable measures to make possible checking and establishing whether and by whom personal data has been entered into data processing systems, modified, or removed. Data Processor will take reasonable measures to ensure that the personal data source is under the control of the Data Controller and the personal data integrated into the Data

Processor's systems is managed by a secure file transfer from the Data Processor and the data subject.

6. Data Backup and Deletion.

Data Processor will ensure that secured backups are conducted on a regular basis and that personal data is encrypted when stored to protect against accidental destruction or loss when hosted by the Data Processor. Date importer will ensure that personal data can be permanently and irretrievably deleted in accordance with industry standards, including by wiping or disposing of storage devices.

7. Logical Separation.

Data Processor will ensure that Data Controller or its clients personal data is logically segregated on Data Processor's systems to ensure that personal data that is collected for different purposes will be processed separately.

8. Additional requirements.

Data Processor will (a) implement detection, prevention, and recovery controls to protect its systems (network, hosting, and application) against malware and other threats to the confidentiality, integrity and availability of personal data, (b) conduct security awareness training to all personnel, and (c) will prohibit and disable the use of non-managed remote devices for storing or carrying, or in use with machines handling personal data Remote devices include without limitation flash drives, CDs, DVDs, external hard drives or other mobile devices.

ANNEX III

LIST OF SUB-PROCESSORS

The same as indicated in the DPA