DATA PROCESSING AGREEMENT TEMPLATE

BETWEEN

MSLA ID, S.L.

as PROCESSOR

AND

[…]

as **SUB-CONTRACTOR**

In […], on […] of […] of […]

This Data Processing Agreement (this "**Agreement**") shall enter into force on […] of […] of […], between:

On the one hand,

(1) **MSLA ID, S.L.**, a company duly incorporated under Spanish law, with registered office at Paseo de la Castellana 18, 7th floor, 28046, Madrid, Spain, and with Tax ID Number B75425579; duly represented by Mr. Luis Emilio Rios Pastrana, of legal age and Peruvian nationality, holder of NIE number Z2501196C, in force, acting as attorney in law for the company (the "**Processor")**.

On the other hand,

(2) **[…].**, a company duly incorporated under the laws of […], with registered office at […] and with Tax ID number […]; duly represented by […], of nationality […] and holder of ID number […], valid, acting as attorney in law for the company (the "**Sub-Processor"**).

Hereinafter, the Controller and the Processor shall be referred to collectively as the **"Parties"** and each of them individually as a **"Party**.**"**

THEY DECLARE

I. That the Processor has been designated by the Controller to carry out certain personal data processing on its behalf, in accordance with the provisions of Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**"GDPR")**, Organic Law 3/2018, of December 5, on Personal Data Protection and Guarantee of Digital Rights ("**LOPDGDD"**).

II. That, for the proper performance of the services entrusted by the Data Controller, the Data Processor needs to rely on the collaboration of third parties acting on its behalf, as sub-processors, under the terms set out in Articles 28.2 and 28.4 of the GDPR.

III. That the Sub-processor has sufficient technical, organizational, and legal capacity to provide the services requested by the Processor, accessing personal data processed by the latter.

IV. That the Parties entered into a service agreement on […] whereby the Subprocessor provides […] services to the Processor (hereinafter referred to as the "**Service Agreement**" and the "**Service**").

V. That both parties wish to regulate by means of this agreement the conditions under which the Subprocessor will carry out the processing of personal data on behalf of the Processor.

VI. That the Parties undertake to comply fully with the obligations established in the GDPR and the LOPDGDD. In particular, the Parties shall implement the security measures required by the GDPR and the LOPDGDD, being personally liable for any penalty, fine or damage that may be imposed on either party as a result of a breach of the obligations provided for in data protection legislation.

VII. That, consequently, the parties agree to sign this data processing agreement, under the terms and conditions established below.

STIPULATIONS

1. DEFINITIONS

1.1 *"Personal data," "processing," "controller," and "data subject*" shall have the same meanings as those established by the GDPR.

1.2 "*Personal Data*" refers to the categories of data owned by the Controller, identified in Annex I, the content of which must be processed by the Processor.

1.3 "*Sub-processor*" means any processor engaged by the Processor or by any other sub-processor who agrees to receive from the Controller or from any other sub-processor the data of the Controller exclusively for the processing activities to be carried out on behalf of the Controller and in accordance with its instructions, under the terms established in this Agreement.

1.4 "*Technical and organizational security* measures" means those measures designed to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against other unlawful forms of processing.

2. DATA PROCESSING

2.1 In accordance with Article 28 of the GDPR, the Processor allows the Subprocessor to access and process the personal data defined in Annex I ("**Personal Data**") that are necessary to provide the Service. This is understood to be without prejudice to the provisions included in the Service Agreement entered into by the Parties regarding personal data.

2.2 For the purposes of this Agreement, the categories of Personal Data may be updated and modified unilaterally, if necessary, by the Processor.

3. OBLIGATIONS OF THE SUB-PROCESSOR

3.1 In accordance with the obligations established in Article 28.3 of the GDPR, the Subprocessor shall comply with the obligations and security measures to ensure compliance with data protection rules. In particular, the Subprocessor undertakes to:

(i) Process personal data only in accordance with the documented instructions of the Processor. If the Processor considers that the instructions received from the Processor violate the rules established by the GDPR, the LOPDGDD or any other applicable regulations, the Processor shall immediately inform the Processor.

(ii) Refrain from applying or using personal data for any purpose other than the fulfillment of this Agreement and the provision of the Service.

(iii) Refrain from disclosing, transferring, or communicating the data in any way to third parties, whether orally or in writing, through electronic means, in writing, or through access by telematic means without the express authorization of the Controller.

To communicate personal data to another Processor acting on behalf of the Processor, the Sub-Processor must follow the instructions of the Processor, and must first identify, in writing, the destination, the categories of data, and the security measures required to carry out the communication.

(iv) The Sub-Processor shall only allow access to the data to its employees when strictly necessary for the provision of the Service and provided that the employees are subject to the same obligations of confidentiality and personal data protection as those established in this Agreement.

(v) If the Sub-processor needs to subcontract the provision of services for the fulfillment of the obligations of the Agreement, it must inform the Processor within fifteen (15) days of such need for subcontracting and provide the details of the subcontracted company, and it will require the authorization of the Processor to carry out a processing assignment by the subcontracted company.

The Sub-Processor shall impose on other sub-processors the same data protection obligations as those established in this Agreement, in particular, it shall provide sufficient guarantees to implement appropriate technical and organizational measures in such a way that the processing complies with the requirements established in the GDPR and the LOPDGDD. Where other sub-processors fail to fulfill their data protection obligations, the Sub-Processor shall remain fully liable to the Processor for the fulfillment of the obligations of the other sub-processors.

(vi) The Sub-Processor shall keep, in writing, a record of the processing activities carried out on behalf of the Processor. This record shall contain the following information:

a) The name and contact details of the Sub-Processor and the Processor on whose behalf it acts, as well as the details of their representatives, if any, and those of the data protection officer;

b) The purpose of the processing and the categories of data subjects and the type of personal data processed on behalf of the Sub-Processor;

c) Transfers of personal data to a third country or international organization, including the identification of that third country or international organization and, in the case of transfers referred to in Article 49(1), second paragraph, documentation of appropriate safeguards;

d) A general description of the technical and organizational security measures.

(vii) The Sub-Processor guarantees to the Processor full compliance with the security measures regarding the type of data obtained. In particular, the security measures included in **Annex** I.

(viii) Assist the Processor through appropriate technical and organizational measures to fulfill the Processor's obligation to respond to requests for the exercise of the data subject's rights, such as the right of access, rectification, erasure, restriction of processing, data portability, and the right to object and automated individual decisions.

When data subjects exercise their rights of access, rectification, erasure, and objection, restriction of processing, data portability, and not to be subject to automated individual decisions, the Processor must notify the Controller immediately, including any information relevant to resolving the request.

(ix) The Deputy Data Protection Officer shall ensure adequate training on data protection for employees who have permanent or regular access to personal data, who participate in the development of tools used to process personal data, or who participate in the collection or processing of personal data.

(x) Assist the Data Controller in implementing a data protection impact assessment.

(xi) Assist the Data Controller in consultations with the supervisory authority.

(xii) Make all information necessary to demonstrate compliance with the obligations established by data protection legislation available to the Controller and allow and contribute to audits, including inspections carried out by the Controller or another auditor ordered by the Controller.

(xiii) The Sub-Processor shall designate a data protection officer in the situations established in Article 37 of the GDPR and communicate their contact details to the Processor.

(xiv) Upon termination of this agreement, the Sub-processor shall return the data to the Processor or destroy it. The Sub-processor may retain the data to prove compliance with legal obligations, as well as any copies or media on which such data is contained, and shall duly certify such return or destruction in writing to the Processor.

4. DATA SECURITY LEVEL

4.1 In accordance with Article 32 of the GDPR, the Sub-Processor shall implement the necessary technical and organizational measures to ensure (i) the pseudonymization 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; and (iv) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

4.2 The Sub-Processor guarantees the adoption of the security measures required in accordance with the GDPR and the LOPDGDD, being personally liable for any penalty, fine or damage that may be imposed for breach of the obligations assumed in this Agreement or those established hereafter by applicable data protection law. In particular, the Sub-Processor shall be liable for any penalties, fines or damages that may arise from the use of personal data for purposes other than those authorized by the Processor, the transfer of data to unauthorized third parties or the irregular use of personal data, as well as if it fails to adopt the appropriate security measures to store, maintain, process and safeguard the data.

4.3 Specifically, the Sub-Processor undertakes to implement the security measures established in **Annex I**.

5. NOTIFICATION OF SECURITY BREACHES

5.1 The Sub-Processor shall notify the Processor, without undue delay, and in any case within a maximum period of 48 hours and via the email address designated for notification purposes, of any breaches of the security of the personal data under its responsibility of which it becomes aware, together with all relevant information for the documentation and communication of the incident.

Notification shall not be necessary where the security breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If available, at least the following information shall be provided:

(i). Description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

(ii). The name and contact details of the data protection officer or privacy officer, or the contact person from whom further information can be obtained.

(iii). Description of the possible consequences of the personal data breach.

(iv). Description of the measures taken or proposed to remedy the personal data breach, including, where appropriate, measures taken to mitigate the possible adverse effects.

If it is not possible to provide information simultaneously, and to the extent that this is not possible, the information shall be provided gradually without undue delay.

6. OBLIGATIONS OF THE PROCESSOR

6.1 The Processor shall ensure that the Sub-Processor guarantees the effective implementation of the GDPR and the LOPDGDD.

6.2 The Processor shall carry out a data protection impact assessment with regard to the processing activities carried out by the Sub-processor.

6.3 It is the responsibility of the Processor to provide the right to information at the time of data collection.

6.4 Consult the supervisory authority prior to processing when necessary.

6.5 Consequently, the Controller shall have the right to carry out monitoring and audit checks to verify that the Sub-processor complies with its obligations.

6.6 In this regard, the Sub-Processor shall, upon request, provide the documentation or information to the Processor so that the Processor can verify such compliance. The Processor may therefore request from the Sub-Processor, with sufficient time for preparation (which must be at least seven days), a certificate of data protection compliance, a copy of the latest audit report, or the implementation of any action that may be required to demonstrate that the Processor fully complies with applicable data protection laws.

7. PROCESSING OF PERSONAL DATA OF REPRESENTATIVES, CONTACT PERSONS, AND OTHER EMPLOYEES OF THE PARTIES

The Parties declare that they are aware that:

(i). That their Personal Data contained in this Agreement and any data that may be collected during the provision of the Service will be processed under the responsibility of each Party for the conclusion, execution, and control of this Agreement and the fulfillment of their respective legal obligations.

(ii). That they may exercise their rights of access, rectification, erasure, objection, portability, and restriction of processing (or any other rights recognized by law) at any time by writing to the relevant party at the addresses indicated in this Agreement and for the attention of the data protection officer or privacy officer.

(iii). That the data protection officers or the privacy officer are responsible for ensuring compliance with data protection regulations.

(iv). That Personal Data will be processed during the term of the Agreement and, thereafter, will remain blocked for the period of limitation of any legal or contractual actions that may apply.

(v). That they may submit any complaint or request related to the protection of Personal Data to the Spanish Data Protection Agency.

Similarly, the Parties undertake to inform the contact persons or other employees whose Personal Data is collected within the framework of this agreement of the processing of all matters referred to in the above points.

8. CONFIDENTIALITY

8.1 The Sub-Processor undertakes to maintain confidentiality with regard to all Personal Data to which the Sub-Processor may have access through any electronic means, documents and/or visual media as a result of this Agreement and the Service Agreement.

8.2 The Subprocessor shall require its employees and the employees of its contractors to maintain confidentiality as set forth in this Agreement and shall provide the Processor with any document confirming compliance with the aforementioned confidentiality obligation.

8.3 The above confidentiality obligations shall remain in force after the termination or expiration of this Agreement or the Service Agreement for any reason. However, such obligations shall not affect information that (i) has been developed independently by the Subcontractor without access to or use of the confidential information; (ii) is made available to the public without the Subcontractor's fault; or (iii) is required to be disclosed by law.

9. LIABILITY

9.1. The Parties agree that, notwithstanding any investigation conducted by or on behalf of the Principal or any knowledge acquired by the Principal at any time, whether before or after the execution and completion of this Agreement or on the date thereof, the Sub-Processor shall be liable and shall indemnify and hold harmless the Processor from and against any penalties, fines, and damages arising directly or indirectly from or in connection with any breach, misrepresentation, inaccuracy, lack of integrity, error or omission of any of its legal obligations as a processor or included in this Agreement or in the Service Agreement, whether voluntary or not, attributable to ordinary negligence or fraud (*"fault, negligence or willful misconduct")* (the "**Damages"**).

9.2. The amount of the Damages shall be calculated by applying the principle of full and complete compensation for all Damages. In the event that the compensation payable by the Sub-Processor has a tax cost for the Processor, the Sub-Processor shall bear the corresponding tax cost and, consequently, the amount of compensation payable to the Processor shall be increased by the amount necessary to neutralize such tax cost.

10. TERM AND TERMINATION OF THE AGREEMENT

10.1 The term of this Agreement is subject to the term of the Services Agreement. Accordingly, upon termination or expiration of the Services Agreement, this Agreement shall automatically terminate.

11. APPLICABLE LAW AND JURISDICTION

11.1 This Agreement shall be governed by and construed in accordance with Spanish law.

11.2 Any dispute arising from this Agreement, or with respect to the validity, interpretation and/or enforcement of this Agreement, shall be referred to the Courts of the city of Madrid, whose award shall be binding on both Parties as final and conclusive.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date above.

On behalf of and in representation of **the MANAGER**

Mr. [*]

On behalf of and representing the **SUB-CONTRACTOR**

_____
Mr. [*]

ANNEX I: PERSONAL DATA

A) Personal

The Personal Data to which the Sub-processor may have access for the performance of the Services provided for in the Agreement are detailed below, including the categories of data subjects and the processing activities:

PURPOSE	Identified in the Agreement
PROCESSING TO BE CARRIED OUT	☐ Collection ☐ Registration ☐ Structuring ☐ Modification/Adaptation ☐ Organization ☐ Extraction ☐ Consultation ☐ Communication by transmission ☐ Dissemination ☐ Interconnection ☐ Comparison ☐ Limitation ☐ Suppression ☐ Destruction ☐ Retention ☐ Communication ☐ Others: .....
PURPOSE OF PROCESSING	☐ Client management, accounting, tax, and administrative purposes ☐ R&D&I, clinical trial research ☐ Pharmacovigilance ☐ Payroll management ☐ Provision of credit and solvency services ☐ Economic, financial, and insurance services ☐ Advertising and commercial prospecting ☐ Guides/directories of electronic communications services ☐ Provision of electronic certification services

	☐ Education ☐ Private security ☐ Video surveillance ☐ Human resources ☐ Occupational risk prevention ☐ Compliance/non-compliance with financial obligations ☐ Profile analysis ☐ Provision of electronic communications services ☐ Training ☐ Management of associative, cultural, recreational, sporting, and social activities ☐ Health ☐ Medical records ☐ E-commerce ☐ Epidemiological research and similar activities ☐ Management of affiliates or members of political parties, trade unions, churches ☐ Social welfare management ☐ Security and access control to buildings ☐ Statistical, historical, or scientific purposes ☐ Other: ……
TYPE OF DATA	☐ Identifying data ☐ Personal characteristics ☐ Academic and professional ☐ Commercial ☐ Social circumstances ☐ Employment details ☐ Financial, economic, or insurance information Business information ☐ Compensation data, employee evaluations ☐ Transactions of goods or services ☐ Password/card details ☐ Special categories of data (ethnic or racial origin, political opinions, religious or philosophical beliefs,

	trade union membership, genetic data, biometric data, health data, data concerning a person's sex life, sexual orientation, criminal convictions and offenses) ☐ Infrastructure data (video surveillance) ☐ Other: ……
CATEGORIES OF DATA SUBJECTS	☐ Employees ☐ Clients and users ☐ Suppliers ☐ Affiliates or members ☐ Owners or tenants ☐ Students ☐ Patients ☐ Healthcare professionals ☐ Contact persons ☐ Parents or guardians ☐ Legal representative ☐ Applicants ☐ Beneficiaries ☐ Public office ☐ Other:

B) Security

The Sub-Processor, with respect to the Personal Data to which it has access during the provision of the service covered by this Agreement, shall comply with the security measures, whether organizational, technical, physical, or administrative, that are appropriate to ensure a level of security appropriate to the risk that may arise from the processing.

In addition, the measures shall guarantee the security, integrity, and availability of Personal Data and prevent its alteration, loss, accidental or unlawful destruction, processing, disclosure, or unauthorized access at all times, taking into account the state of the art, the costs of implementation, the nature of the data stored, the scope of the processing, as well as the risks to which they are exposed and the impact this could have on the rights and freedoms of natural persons.

The planning of security measures must include the implementation of mechanisms that allow for the rapid restoration of availability and access to Personal Data in the event of a physical or technical incident.

The Sub-Processor shall adopt at least the following technical and organizational security measures:

(i) Appointment of a data protection officer, either a data protection delegate or a designated privacy officer, who shall ensure compliance with applicable regulations.

(ii) Establishment of roles and responsibilities for personnel who process Personal Data.

(iii) Communication between staff members regarding the defined roles and responsibilities associated with compliance with data protection regulations.

(iv) Definition of roles and profiles for users of applications and systems where such data is processed in accordance with the established functions and responsibilities, so as to prevent access to data or resources other than those authorized. This access control system must guarantee adequate user identification and authentication mechanisms, such as the use of passwords that must be renewed periodically, the use of biometric data, automatic user blocking after successive failed access attempts, etc.

(v) Automated measures that restrict access to information for unauthorized users or users outside the specified retention period, such as data erasure or pseudonymization techniques.

(vi) Procedures that limit physical access to the facilities where the information systems or physical media are located.

(vii) Control and access logs on media containing Personal Data, which must also have limited access mechanisms.

(viii) Procedures for recovering Personal Data in the event of its destruction, loss, or alteration, under the supervision and approval of the data protection officer.

(ix) Procedures for detecting, assessing, and reporting security incidents that may affect the rights and freedoms of individuals.

(x) Periodic compliance reviews and definition and implementation of action plans to mitigate detected risks.

If the Personal Data is specially protected, the Sub-Processor shall implement at least the following additional measures:

(i) Provide a log of access to particularly sensitive data in which the user and date of access can be identified.

(ii) Encryption, data encryption, or similar measures on physical media and portable devices containing particularly sensitive data that are sent or used outside the company's premises.

(iii) Encryption or coding of particularly sensitive data transmitted via electronic networks.

(iv) Measures to prevent access to particularly sensitive data on physical media (e.g., documentation) during its transfer from the company's premises to its storage location, which in turn must have adequate access control measures in place.