DATA PROCESSING AGREEMENT

Both referred to jointly as "the Parties," acknowledging sufficient capacity for the execution of this agreement,

STATE

That, within the framework of providing the Services, the Provider may require access to personal data, as defined in Regulation (EU) 2016/679, General Data Protection Regulation (hereinafter "GDPR").

That, in order to comply with the obligation imposed by Article 28 of the GDPR, both Parties agree to sign this Data Processing Agreement, which governs, as a framework agreement, the processing of personal data on behalf and for the account of the CONTROLLER, derived from any services requested and contracted from the PROCESSOR, which includes the following

TERMS

1. Scope of Processing

In addition to what is established in the Purchase Order, the scope of the processing of personal data derived from any services requested and contracted from the PROCESSOR includes the following terms:

Categories of Data Subject to Processing:

The data subject to processing will be those identifying or contact details necessary for the correct provision of the services specified in the Purchase Order, such as name, surname, email, phone number, etc. Additionally, other categories of personal data may be subject to processing:

- Employment details (profession, category…)
- Economic data (financial data, bank account)
- Employee data
- Supplier data
- Customer data

Categories of Data Subjects:

The categories of data subjects whose data will be processed will be those necessary for the correct provision of the services specified in the Purchase Order.

Authorized Processing Operations:

The authorized processing operations will be those necessary for the correct provision of the services specified in the Purchase Order.

2. Obligations of the PROCESSOR

The PROCESSOR will carry out the processing of personal data derived from the provision of the contracted Services, in accordance with the following obligations:

- Limit actions to those necessary to provide the CONTROLLER with the Services, adhering to the instructions given by the CONTROLLER at all times, including with respect to the transfer of personal data to a third country or an international organization, unless required by legal obligation, in which case, the CONTROLLER will be informed of such legal requirement prior to processing.

- If the PROCESSOR believes that any instruction violates current legislation, they must immediately inform the CONTROLLER.
- Commit not to perform any other processing on the personal data, nor to apply or use the data for any purpose other than the provision of the Services, nor to use them for their own purposes.
- Guarantee the necessary training on personal data protection for authorized persons processing personal data.
- Maintain a written record of all processing activities carried out on behalf of the CONTROLLER, containing the information required by Article 30 of the GDPR. ● Commit to keep under their control and custody the personal data accessed due to the provision of the Services and not to disclose, transfer, or otherwise communicate them, not even for their storage, to other persons.
- If required to transfer personal data to a third country or an international organization under Union or Member State law applicable to the PROCESSOR, inform the CONTROLLER of this legal requirement prior to processing, unless the law prohibits such information for important public interest reasons.
- Support the CONTROLLER in conducting data protection impact assessments and prior consultations with the supervisory authority, when applicable.
- Provide the CONTROLLER with all necessary information to demonstrate compliance with their obligations, and collaborate in audits or inspections conducted by the CONTROLLER or another auditor authorized by them.
- The CONTROLLER may visit the PROCESSOR's facilities and, if applicable, those of any subcontractors, with prior notice of five (5) business days, to conduct the necessary on-site checks and audits to verify compliance with current regulations. The maximum number of on-site audits will be one per calendar year unless a legitimate interest in greater frequency is proven. The Parties will agree on the conditions of their execution (e.g., scope, resources allocated, and, if applicable, conditions for contracting an independent third-party auditor).
- Appoint a data protection officer, when required, and communicate their identity and contact details to the CONTROLLER.
- Notify the CONTROLLER without undue delay, and in any case within a maximum of forty-eight (48) hours, of any personal data breaches under their control, including all relevant information for documenting and reporting the incident, providing at least: a description of the nature of the personal data breach, the contact point where more information can be obtained, an analysis of the possible consequences of the personal data breach, and a description of the measures taken or proposed to mitigate the possible negative effects. If it is not possible to provide the information simultaneously, it will be provided gradually without undue delay.
- Assist the CONTROLLER in responding to the exercise of data subjects' rights, providing the necessary information for the proper resolution of the request. If the PROCESSOR receives any request to exercise rights, they will forward it to the CONTROLLER without undue delay and, at the latest, within three (3) calendar days from its receipt, for proper resolution.

3. Security of Personal Data

The PROCESSOR declares to be aware of the obligations arising from data protection regulations, especially regarding the implementation of security measures for different categories of data and processing established in Article 32 of the GDPR.

- The PROCESSOR guarantees that these security measures will be properly implemented and will help the CONTROLLER comply with the obligations set out in Articles 32 to 36 of the GDPR, considering the nature of the processing and the information available to the PROCESSOR.
- The CONTROLLER will conduct an analysis of the potential risks derived from the processing to determine the appropriate security measures to ensure the information's security and the data subjects' rights. If risks are identified, they will provide the

PROCESSOR with a risk assessment report to implement appropriate measures to avoid or mitigate them.

- The PROCESSOR, in turn, will analyze potential risks and other circumstances that may affect security and inform the CONTROLLER of any they identify for impact evaluation.
- The PROCESSOR guarantees that, considering the state of the art, the implementation costs, and the nature, scope, context, and purposes of the processing, they will implement appropriate technical and organizational measures to ensure a security level appropriate to the risk of processing, which may include, among others:
    - Pseudonymization and encryption of personal data.
    - Ensuring the confidentiality, integrity, availability, and resilience of processing systems and services.
    - Restoring the availability and access to data quickly in case of a physical or technical incident.
    - Regularly verifying, evaluating, and assessing the effectiveness of technical and organizational measures to ensure processing security.

4. Confidentiality

The PROCESSOR is obliged, in compliance with data protection regulations and the duty of professional secrecy, not to disclose information to third parties regarding the data they access and process to provide the Services. This duty of confidentiality will remain over time, even after the contract ends.

- If a judicial authority contacts the PROCESSOR to request information from the CONTROLLER, the PROCESSOR will try to prompt the competent authority to request the information directly from the CONTROLLER. If the PROCESSOR is obliged to disclose such information to the authority, they will immediately notify the CONTROLLER, providing a copy of the request.
- The PROCESSOR will also ensure that persons authorized to process personal data expressly and in writing commit to confidentiality and comply with the corresponding security measures, which the CONTROLLER will inform appropriately.

5. Obligation to Return or Destroy Data

Once the service is completed, the PROCESSOR commits to securely destroy any information containing personal data transmitted by the CONTROLLER for the provision of the Services. To do so, they will apply appropriate physical and logical measures to ensure that the data incorporated into different media are irrecoverable. Subsequently, they will issue a secure destruction certificate to the CONTROLLER identifying the information, physical media, and/or documents destroyed.

- Notwithstanding the above, prior to their destruction, the PROCESSOR will offer the return of the data to the CONTROLLER, which will involve delivering or making the data available in a commonly used format, ensuring that the CONTROLLER does not depend on the PROCESSOR's systems or tools. After the return process is completed, the PROCESSOR will securely destroy the data, as established in the previous paragraph.
- In any case, the PROCESSOR may retain the data properly blocked in case of potential liabilities from their relationship with the CONTROLLER, proceeding to their destruction once the statute of limitations for actions expires.

6. Subcontracting

The PROCESSOR may not subcontract with third parties for the provision of the Services without the express prior written authorization of the CONTROLLER.

- In this regard, the CONTROLLER expressly authorizes the PROCESSOR to subcontract with the following third parties:

Provider	Service	Local/international data transfers
Google Cloud Platform	Cloud storage	Germany, UE
MongoDB	Data base	UE
Hubspot	Inbound marketing	UE
Bigquery	Data base	UE
Identity Platform	Access control	UE
Zendesk	Client support	UE

- Nevertheless, the CONTROLLER will generally authorize the PROCESSOR to subcontract all or part of the Services as long as they notify the CONTROLLER, in advance, expressly, and in writing, about the identity of the subcontractor and the service subject to subcontracting. The CONTROLLER may oppose such subcontracting within ten (10) business days from the notification made by the PROCESSOR.
- It is the initial PROCESSOR's responsibility to regulate the new relationship in accordance with Article 28 of the GDPR, so that the subcontractor (the "SUB-PROCESSOR") is subject to the same conditions (instructions, obligations, security measures...) and formal requirements as the PROCESSOR concerning the proper processing of personal data and ensuring the rights of affected individuals, established by regulations and in this contract.
- In the case of non-compliance by the SUB-PROCESSOR, the initial PROCESSOR will remain fully responsible to the CONTROLLER regarding the fulfillment of obligations.

7. Data Location and International Transfers

The transfer of personal data to third countries outside the European Economic Area is not generally authorized, except as provided in the previous clause.

- If an international transfer of the data subject to processing is required, (i) the PROCESSOR must obtain the CONTROLLER's prior and express written authorization, as well as (ii) ensure compliance with the provisions of Chapter V of the GDPR.
- In this regard, if the international transfer of the data is authorized, it must be carried out (i) either to the territory of a country for which the European Commission has adopted an Adequacy Decision, or (ii) by adopting appropriate safeguards according to the options recognized by Article 46 of the GDPR, preferably through the adoption of standard contractual clauses approved by the European Commission, included as Annex 1.

8. Responsibilities

In accordance with Article 28.10 of the GDPR and other data protection regulations, if the PROCESSOR violates the GDPR by determining the purposes and means of processing, they will be considered the controller regarding that processing, and must indemnify the CONTROLLER for any damage caused by non-compliance with their legal and contractual obligations.

9. Data Processing as Sub-Processor

If, in the provision of the Services, the CONTROLLER communicates data to the PROCESSOR for which the former also acts as a processor, the PROCESSOR will process them according to the terms agreed in this agreement and will be considered a sub-processor in relation to them.

10. Entry into Force

This agreement enters into force on the date of its signing and will remain in effect until the termination date of the contractual relationship whose object is the Services, without prejudice to the survival of all those obligations (such as the obligation to return and/or destroy the data) which, according to their nature or the terms of this agreement, should survive its termination, as well as any other legal obligation applicable to the parties after the termination of that relationship.

Anexo 1. SSC (Processor to Processor).pdf

Anexo 1. CCT (Controller to Processor).pdf