# DATA PROCESSING AGREEMENT

On one hand, the client, hereinafter DATA CONTROLLER, and on the other hand GCON4 SPAIN SL, hereinafter DATA PROCESSOR, with domicile at CL Alameda Urquijo 45 1º izquierda 48011 – Bilbao (Bizkaia) and email address info@gcon4.com. Both parties, hereinafter individually referred to as "the Party" and collectively as "the Parties", declare that their powers are in force and have not been altered, recognizing themselves, consequently, with sufficient legal capacity to grant this, DATA PROCESSING AGREEMENT (hereinafter, the Agreement), and, to this end, STATE: I. - That the Parties have signed a service provision agreement described in Annex I (hereinafter the Main Agreement).II. - That for the provision of the services object of the Main Agreement, it is necessary for the DATA PROCESSOR to carry out a series of data processing identified in Annex I on behalf of the DATA CONTROLLER. III. - That, for this reason and in compliance with Article 28 of Regulation 2016/679 (hereinafter GDPR), and Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights, both Parties of their free and spontaneous will agree to regulate this access and processing of personal data in accordance with the following CLAUSES.FIRST – OBJECT:1.1.- This agreement aims to regulate the conditions of the processing indicated in the preamble of this Agreement by the DATA PROCESSOR. For appropriate purposes, Annex I states the object, duration, nature, and purpose of the processing, as well as the type, categories of data, and processing operations to be carried out. SECOND - PROCESSING BY THE PROCESSOR IN ACCORDANCE WITH THE INSTRUCTIONS OF THE DATA CONTROLLER. 2.1.- The PROCESSOR will process the personal data provided by the DATA CONTROLLER solely and exclusively following the documented instructions provided by the DATA CONTROLLER. Compliance with the instructions of the DATA CONTROLLER must also occur in the case of international data transfers that may occur as a result of the service provision, unless required by Union or Member State law applicable to the PROCESSOR. In such a case, the PROCESSOR will inform the DATA CONTROLLER of this legal requirement prior to processing, unless such law prohibits it for important public interest reasons. 2.2.- If the DATA PROCESSOR considers that any of the instructions provided violates data protection regulations, the PROCESSOR will immediately inform the DATA CONTROLLER of this circumstance, being in any case obliged to comply with the applicable regulations. 2.3.- In the event that the DATA PROCESSOR determines the purposes and means of the processing, it will be considered responsible for the purposes of data protection regulations, thus being subject to the legal responsibilities that may arise in this regard. THIRD. - ON PERSONNEL WITH ACCESS TO DATA: CONFIDENTIALITY AGREEMENTS. The DATA PROCESSOR must maintain the utmost confidentiality regarding the personal data subject to processing and commits and obliges that all personnel under its responsibility who will process the data subject to this Agreement have previously signed a confidentiality agreement. It will not be necessary to sign the confidentiality agreement for those persons subject to a statutory confidentiality obligation. 3.2.- The DATA PROCESSOR will take appropriate measures to ensure that any person acting under its authority and having access to personal data has the necessary skills, training, and instructions to carry out the processing under the instructions provided by the DATA CONTROLLER to the PROCESSOR. FOURTH. - DATA SECURITY. RISK ANALYSIS. 4.1.- For the purposes of complying with Article 32 of the GDPR, the PROCESSOR will apply appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, implementation costs, and the nature, scope, context, and purposes of the processing, as well as risks of varying probability and severity for the rights and freedoms of natural persons. For appropriate purposes, Annex I lists the measures to be adopted by the DATA PROCESSOR. 4.2.- In any case, the DATA PROCESSOR commits and obliges to adopt a regular process of verification, evaluation, and assessment of the effectiveness of technical and organizational measures to ensure the security of the processing. FIFTH. - IMPACT ASSESSMENT AND PRIOR CONSULTATION. 5.1.- In the event that Article 28.3 f) of the GDPR applies, the PROCESSOR will assist the RESPONSIBLE in carrying out and maintaining the impact assessments and prior consultation established in the regulations, taking into account the nature of the processing and the information available to the PROCESSOR. SIXTH. - SECURITY BREACHES. 6.1.- The DATA PROCESSOR will notify the DATA CONTROLLER without undue delay of any security breaches of personal data under its charge that it becomes aware of, along with all relevant information for documenting and communicating the incident. The DATA PROCESSOR will notify, at a minimum, the information contemplated in Article 33.3 of the GDPR. If it is not possible to provide the information simultaneously, the DATA PROCESSOR commits to providing it gradually without undue delay. 6.2.- Upon occurrence of the security incident, the DATA PROCESSOR will carry out the necessary actions to investigate, mitigate, and remedy the incident, and will promptly inform the DATA CONTROLLER of the progress and results of these actions. SEVENTH. - DESTINATION OF DATA ONCE THE PROCESSING SERVICES ARE COMPLETED. 7.1.- Depending on what is indicated in Annex I, the DATA PROCESSOR will return to the RESPONSIBLE (or the processor designated by the DATA CONTROLLER) or delete all personal data once the processing services are completed, unless according to some legal norm it is necessary to retain them. 7.2.- Notwithstanding the provisions of the previous section, the DATA PROCESSOR may retain the data duly blocked while any type of liability may arise from the services provided. EIGHTH. - SUB-PROCESSORS. 8.1.- The PROCESSOR may not engage another processor (hereinafter, the SUB-PROCESSOR) to carry out the processing activities covered by this contract, unless there is specific or general prior written authorization from the CONTROLLER. The PROCESSOR must evaluate the SUB-PROCESSOR in advance to verify that it meets the necessary guarantees for the processing and must adequately document all of this. For appropriate purposes, the CONTROLLER may at any time expressly indicate, via email (info@gcon4.com), the processors to whom the PROCESSOR may resort. 8.2.- In the event that the CONTROLLER authorizes subcontracting, the PROCESSOR will sign a contract with the SUB-PROCESSOR in which the latter will be imposed at least the same data protection obligations stipulated in this Contract for the PROCESSOR and, in particular, the provision of sufficient guarantees for the application of appropriate technical and organizational measures so that the processing complies with the provisions of the data protection regulations. If, given the circumstances, it is necessary to adopt new measures or intensify existing ones, the PROCESSOR must require these measures from the SUB-PROCESSOR in the contract or during the relationship. 8.3.- At the request of the CONTROLLER, the PROCESSOR will provide the necessary information for the CONTROLLER to comply with Article 28.3. h) of the GDPR. Upon request from the CONTROLLER, the PROCESSOR will send the contracts signed with the SUB-PROCESSORS as well as any information that proves the existence of guarantees and their evaluation by the PROCESSOR. 8.4.- If the SUB-PROCESSOR fails to comply with its data protection obligations, the PROCESSOR will be fully responsible to the CONTROLLER for the fulfillment of the new processor's obligations. NINTH. - REPRESENTATIONS AND WARRANTIES. ACCREDITATION OF COMPLIANCE WITH DATA PROTECTION OBLIGATIONS. NOTIFICATIONS. 9.1.- The DATA CONTROLLER declares that all personal data to be processed by the PROCESSOR have been or will be legally obtained from the data subjects. In this regard, the DATA CONTROLLER will be strictly responsible for compliance with the lawfulness of processing obligations set forth in the regulations and, in particular, for providing the right to information to the data subjects at the time of data collection or at a later time (if the data have not been obtained from the affected individuals). 9.2.- The DATA PROCESSOR expressly declares that it meets sufficient guarantees for compliance with data protection regulations and, in particular, regarding the application of technical and organizational measures that meet the requirements of the GDPR. 9.3.- The DATA PROCESSOR will make available to the DATA CONTROLLER all necessary information to demonstrate compliance with the obligations established in this Agreement. The DATA PROCESSOR commits and obliges to allow and contribute to audits, including inspections, by the DATA CONTROLLER or another auditor authorized by the DATA CONTROLLER. 9.4.- Communications arising from this Agreement will be made to the addresses and/or persons indicated in Annex I. TENTH. - EXERCISE OF RIGHTS: ASSISTANCE OF THE PROCESSOR TO THE DATA CONTROLLER. 10.1.- The DATA PROCESSOR will assist the DATA CONTROLLER, taking into account the nature of the processing, through appropriate technical and organizational measures, whenever possible, so that the DATA CONTROLLER can comply with its obligation to respond to requests aimed at exercising the rights of the data subjects established in the GDPR. 10.2.- For the purposes indicated in the previous section, the Parties agree that when the affected individuals exercise their rights of access, rectification, deletion, and opposition, limitation of processing, data portability, and not being subject to automated individual decisions before the DATA PROCESSOR, the DATA PROCESSOR must communicate it to the DATA CONTROLLER. The communication must be made immediately and in no case beyond the next business day after receiving the request, along with, if applicable, other information that may be relevant to resolve the request. ELEVENTH. - PRIVACY POLICY. This privacy policy applies to the collection of data by each of the Parties regarding the processing of data of the natural persons involved in it. For clarification purposes, it is stated that in no case is the data processing joint, with each Party being responsible for compliance with its data protection obligations. 11.1- Purpose of processing. Control and execution of this Agreement.11.2. - Legal basis for processing. The execution of this Agreement or, in the case of a natural person acting on behalf and representation of another, based on legitimate interest. (Art. 6.1.b) and 6.1.f) in relation to Article 19 of Organic Law 3/2018, respectively of the General Data Protection Regulation or GDPR).11.3. - Retention periods. While the duration of this agreement is maintained and once it is completed, until the end of any periods arising from compliance with legal obligations, including any prescription periods. 11.4. - Communications and/or transfers. Unless legally required, each of the responsible parties informs that the data of the natural person representative will not be transferred to any third party without their consent, unless such communication is necessary for the execution of this agreement.11.5. - Rights of the data subject. The data subject has the possibility to exercise the rights of access, rectification, deletion, portability, limitation, or opposition. The exercise of these rights may be made by written request to the responsible party at the contact address indicated in the first section of this clause, in the terms subscribed by current legislation. Likewise, a complaint may be filed with the competent supervisory authority, exercising this function in Spain the Spanish Data Protection Agency (www.aepd.es). TWELFTH. – JURISDICTION 12.1.- For the resolution of any discrepancy resulting from the interpretation or execution of this agreement, the Parties expressly submit to the jurisdiction and competence of the Courts and Tribunals indicated in the Main Agreement, expressly waiving any other jurisdiction that may correspond to them.

## ANNEX I

INFORMATION ABOUT THE PROCESSING:

Object, duration, and nature of the processing: according to the provisions of the Main Agreement.

Purpose of the processing: Manage the relationship with clients. Send commercial communications.

GENERAL DESCRIPTION OF PROCESSING:

At the end of the processing: The DATA CONTROLLER may indicate through digital or physical means whether they wish the data to be returned to the DATA CONTROLLER or to another processor they designate. Alternatively, they may request the destruction of the data.

TYPE OF DATA: Identifying data.

CATEGORIES OF DATA SUBJECTS: Clients and users; Contact persons; Legal representative.

SPECIFICATION OF THE PROCESSING TO BE CARRIED OUT: Collection (data capture); Consultation.

SECURITY MEASURES TO BE ADOPTED BY THE DATA PROCESSOR:

Security controls indicated in ISO 27002:2022 according to the statement of applicability. Safeguards related to the National Security Scheme corresponding to the security category of the information system BASIC/MEDIUM/HIGH.

Backup and restoration procedures:

The DATA PROCESSOR must have a backup system that includes the following aspects:

- The procedure must be documented, and incidents must be recorded.
- Supervision and monitoring of this procedure will be carried out, with verification alerts as appropriate. Periodically, a restoration test must be performed to verify the system.
- If backups are made to external media, these media must be inventoried and encrypted, with security measures implemented to ensure proper preservation and access control.

Assets | Information classification and access controls:

The DATA PROCESSOR must have the system security assets inventoried, under control, and supervision. The DATA CONTROLLER's information must be identified and separated from the rest of the DATA PROCESSOR's data and information. Appropriate physical and logical access control measures must exist for the assets.

- Workstation | The DATA PROCESSOR must have the following measures:
- Updated antivirus.
- Operating systems and programs with manufacturer security support and updated with the latest patches.
- Limitation of permissions and applications that users can install.
- Hard disk encryption.
- Device access control.
- Automatic screen lock during inactivity.
- Enabled firewall.

If remote access is necessary, it must be encrypted with a solution that ensures the confidentiality of the information.

Networks and communications:

- Perimeter firewall.
- All network elements must have an adequate security policy, which includes that access to them for management and administration is done through a secure channel.
- If remote access exists, it must be done via VPN or similar.
- If wireless networks exist, they must be encrypted and adequately isolated and/or secured.

Security updates: The DATA PROCESSOR must keep all systems that process personal data updated with the latest patches and updates from the manufacturer. This includes operating systems, programs, etc., but also other elements such as mobile phones, network elements (e.g., switches, routers, firewalls, etc.), printers, etc.

External security audit: Periodically, the DATA PROCESSOR will undergo a security audit to evaluate the general privacy program, and particularly the DATA PROCESSOR's information security management system.

Security incidents and data security breaches: The DATA PROCESSOR must have a security incident management protocol that allows the identification, adoption of appropriate mitigation and corrective measures, as well as the proper management and notification of these incidents to the DATA CONTROLLER.

Rights exercise management protocol: The DATA PROCESSOR must have a system to manage the rights exercises that affected individuals may carry out.

Media and supports: The DATA PROCESSOR must have appropriate protocols to ensure the inventory and traceability of the media and supports that process data. It must have policies and procedures that allow the proper elimination of data in case of reuse of the support or an appropriate protocol for the destruction of the support or medium.

Personnel: The DATA PROCESSOR must develop a training, education, and awareness program for its personnel. This program must include at least one annual training session and must cover general data protection issues, protocols associated with data processing, as well as the technical and organizational measures that they must know and/or apply.

LIST OF SUB-PROCESSORS: GCON4 COLOMBIA SAS with domicile at CRA 6 # 67-09 Office 402 Bogotá D.C – Colombia. Processing: Consultation.