Data Processing Agreement (DPA)

PROCESSOR

Form.taxi – Reinhard Söllradl
Brandstatt 9
4070 Eferding
Austria

CUSTOMER

Carlos León Bolaños
Calle Hermano Pedro, 4
38010 Santa Cruz de Tenerife
España

Preamble and Scope of Application

The Processor is commissioned by the Customer to process personal data on behalf of the Customer. The DPA specifies this processing with regard to its object and the rights and obligations between the Contracting Parties arising from the Processing.

1. Terms and Definitions

3. "Processing" – Pursuant to 4 (8) GDPR, "Processing" is understood to mean the processing of personal data as defined in Article 4 (2) GDPR carried out on behalf of the Controller, irrespective of the number of intermediary processors, by the Processor in accordance with the subject-matter of this DPA.
4. "Principal Agreement" – The term "Principal Agreement" covers all types of ongoing business relations between the Customer and the Processor, under which the Processor processes personal data at the instruction of the Customer in accordance with the definition of the subject of the Processing in this DPA. Insofar as the validity of this DPA is otherwise limited (i.e. within this agreement or outside it, in other agreements or regulations) to certain types, categories or specific business relationships, contracts, etc., these are each to be understood as the Principal Agreement. The definition of the Principal Agreement also includes ongoing individual assignments by the Customer to the Processor, which are issued by the Customer within the scope of the Principal Agreement (e.g. in the case of framework contracts).
5. "Personal Data" – In accordance with Article 4 (1) GDPR, "personal data" (hereinafter also referred to briefly as "data") is all information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
6. "Third party" – "Third party" means according to Article 4 (10) GDPR a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
7. "Sub-processing" – When a processor is not directly appointed by the Controller but by a processor who is the first processor appointed by the Controller, a "sub-processing" is present and the processors following the first processor are referred to as "sub-processors".

2. Type of Processing

8. Insofar as the Customer acts as the Controller of the Processing, it shall be responsible within the scope of this DPA for compliance with the provisions of the data protection laws, in particular for the legality of the Data Processing as well as for the legality of the assignment of the Processor. Insofar as the Customer itself acts as a Processor, the Customer shall commission the Processor as a Sub-Processor. The controller of the processing may, on the basis of this DPA, directly invoke the rights to which the Customer is entitled to against the Sub-Processor.

3. Authority to issue instructions

9. The Processor may process Data only within the scope of the Principal Agreement and of the Customer's instructions and only insofar as Processing within the scope of the Principal Agreement is necessary.

10. The Processor may be obliged to carry out processing operations or to communicate information by Union or Member State law and by administrative and judicial measures to which the Customer is subject. In such a case, the Processor shall communicate the legal requirements of the overriding legal obligation to the Customer prior to the processing, unless the law or order in question prohibits such communication on the grounds of an important public interest; in the event of a prohibition on communication, the Processor shall take possible and reasonable measures to prevent or restrict the legally overriding Processing.

4. Technical and Organisational Measures (Safety and Security Concept)

11. The Processor shall structure the internal organisation in his area of responsibility in accordance with the legal requirements and shall in particular implement technical and organisational measures (hereinafter referred to as "TOMs") for appropriate security, in particular the confidentiality, integrity and availability of the Customer's Data, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the Processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of the persons concerned, and shall ensure that these measures are maintained, in particular by means of regular evaluation, at least once a year. With regard to the protection of the Data, the TOMs include in particular physical and logical access control, transfer control, input control, order control, integrity and availability control, separation control and the safeguarding of the rights of the Data Subjects.

12. The Processor shall ensure that the employees, agents and other persons acting on behalf of the Processor are prohibited from processing the Data outside the scope of the Instruction. The Processor shall further ensure that the persons authorised to process the Client's Data have been instructed in the data protection provisions of law and of this DPA and have been bound to confidentiality and secrecy or are subject to a corresponding and appropriate legal obligation of secrecy. The Processor shall ensure that the persons employed for the Processing are with regard to the fulfilment of the data protection requirements appropriately instructed and supervised on an ongoing basis.

13. If required by law, the processor shall appoint a data protection officer in accordance with the legal requirements. The Processor shall inform the Customer of the contact details of the data protection officer and of any subsequent changes.

14. If the security measures taken do not or no longer meet the requirements of the Customer or the statutory requirements, the Processor shall notify the Customer immediately.

5. Information and cooperation obligations of the processor

15. The Processor may only provide information to third parties or the data subjects with the prior approval of the Customer. If a data subject contacts the Processor and asserts his or

her rights as data subject (in particular rights of access or rectification or deletion of personal data), the Processor shall refer the data subject to the Customer, provided that, according to the data subject, an attribution to the Customer is possible. The Processor shall immediately forward the request of the data subject to the Customer and shall support the Customer within the scope of reasonableness and possibility. The Processor shall not be liable if the request of the data subject is not, not correctly or not timely answered by the principal, unless the Processor is responsible for this shortcoming.

16. The Processor shall immediately and fully inform the Customer if, with regard to the Processing, the Processor discovers errors or irregularities in the compliance with the requirements of this DPA and/or relevant data protection provisions. The Processor shall take the necessary measures to secure the Data and to mitigate any adverse consequences for the data subjects and shall consult with the Customer without delay.
17. The Processor shall inform the Customer without delay if a supervisory authority takes action against the Processor and whose activities may affect the Data processed for the Customer. The processor shall support the Customer in the fulfilment of his/her obligations (in particular to provide information and allow inspections) with regard to supervisory authorities.
18. Should the security of the Data be endangered (seizure, confiscation, insolvency proceedings, etc.) by measures taken by third parties (e.g. creditors, authorities, courts, etc.), the Processor shall inform the third parties without delay that the sovereignty and ownership of the Data lies exclusively with the Customer and, after consultation with the Customer, shall take appropriate protective measures (e.g. lodge objections, applications, etc.) if necessary.
19. The Processor shall provide the Customer with information relating to the Processing which is necessary for the fulfilment of the Customer's legal obligations (which may include, in particular, requests from data subjects or authorities and compliance with the Customer's accountability obligations of a data protection impact assessment) and shall assist the Customer in complying with the obligations set out in Articles 32–36 GDPR.
20. The obligations of the Processor to provide certain information shall initially extend to information available to the Processor, his/her employees and agents. The information need not be obtained from third sources if the procurement by the Customer could be carried out within reasonable limits and no other agreement has been made.

6. Measures in the Event of a threat to Data Protection or Data Breach

21. In the event that the Processor becomes aware of facts which give rise to the assumption that the protection of the processed Data may have been breached within the meaning of Article 4 (12) GDPR, the Processor shall inform the Customer without delay and in full, take the necessary protective measures without delay, and assist the Customer in the performance of the Customer's obligations, in particular in relation to the notification of competent authorities or data subjects.
22. The notification from the Processor must according to Article 33 (3) GDPR contain at least the following information:

    - description of the nature of the data breach or threat, specifying, where possible, the

categories of data concerned and the approximate number of persons and personal data sets concerned;

- the name and contact details of the data protection officer or any other known contact point for further information;
- a description of the likely consequences of the data breach or threat (e.g. with further details: identity theft, financial loss, etc.);
- a description of the measures taken or proposed by the Processor to remedy the data breach and, where appropriate, measures to mitigate its possible adverse effects

7. Sub-Processing

23. The Controller, notwithstanding any restrictions arising from the Main Agreement, expressly consents to the Processor engaging sub-processors within the scope of the processing.

24. The Processor shall inform the Controller of any intended change concerning the addition or replacement of sub-processors. Such information shall be provided actively and in text form (in particular by email to a contact address designated by the Controller) in good time prior to the change taking effect, as a rule at least two (2) weeks in advance. The Controller may object to the intended change within two (2) weeks of receipt of the information on important grounds relating to data protection. If the Controller does not object within this period, the change shall be deemed approved. In the event of an objection, the parties shall seek to reach an amicable solution. If no such solution can be reached, the Controller shall be entitled to terminate the affected Main Agreement.

25. If the processor uses the services of a sub-processor (e.g. a subcontractor) in order to carry out certain Processing activities on behalf of the Customer, it must impose on the sub-processor, by means of a contract or any other legal instrument permitted by law, the same data protection obligations as those to which the Processor has committed him/herself in this DPA (in particular as regards following instructions, complying with the TOMs, providing information and allowing audits).

26. Processing of personal data which is not directly related to the provision of the main contractual obligation and where the Processor uses the assistance of third parties as a mere ancillary service in order to carry out its business activity (e.g. cleaning, security, maintenance, telecommunications or transport services) does not constitute sub-processing within the meaning of the above provisions of this DPA. Nevertheless, the processor shall ensure, e.g. by contractual agreements or notices and instructions, that the security of the data is not endangered and that the provisions of this processing contract and the data protection regulations are observed.

27. The sub-processor shall be carefully selected by the Processor, having particular regard to the suitability and reliability of the sub-processor to comply with the obligations under this DPA for Processing and the adequacy of the TOMs implemented by the sub-processor.

28. The responsibilities for performing the obligations under this DPA and under the law must be clearly defined and allocated between the processor and the sub-processor.

29. The sub-processing relationships already in existence at the time of the conclusion of this DPA are listed by the Processor in the Annex "Sub-Processors" and updated by the Processor.

8. Spatial Area of the Processing

30. Processing may take place in third countries provided that the special conditions laid down in Article 44 et seq. GDPR are fulfilled, i.e. in particular a) the EU Commission has established an adequate level of data protection; or b) on the basis of so-called Standard Contractual Clauses (SCC); or c) on the basis of binding corporate rules.

9. Obligations of the Customer

31. In the event of a claim against the Processor by data subjects, third parties, bodies or authorities with regard to possible entitlements arising from the processing of the Data within the scope of this DPA, the Customer undertakes to support the Processor in the defence of the claim within the scope of its possibilities and taking into account the degree of fault of the Contracting Parties.

10. Liability

32. The statutory liability provisions apply, in particular Article 82 GDPR and, in the case of the use of a sub-processor, Article 28 (4) S. 2 GDPR.

11. Term, Continuation after Termination of the DPA and Deletion of Data

33. Upon completion of the Processing under this DPA, the Processor shall destroy all Data and copies thereof (as well as all documents, processing and usage results and data files coming into its possession in connection with the contractual relationship), unless there is a legal obligation to store the Data, in which case the Processor shall inform the Customer of the obligation and its scope, unless the Customer can be expected to be aware of the obligation. The destruction or deletion must be carried out in accordance with data protection regulations and in such a way that a recovery of even residual information is no longer possible or cannot be expected with reasonable effort. The objection of a right of retention is excluded with regard to the processed Data and the associated data carriers. With regard to the deletion, the rights of the Customer to information, proof and audit apply in accordance with this DPA.

34. The effective term and termination of this DPA shall be determined by the term and termination of the Principal Agreement.

35. The termination of the Agreement, as well as the termination of this clause must be made at least in electronic format.

36. The obligations to protect confidential information arising from the DPA shall continue to apply after the end of the DPA, provided that the Processor continues to process the Personal Data covered by the DPA and that compliance with the obligations can reasonably be expected of the Processor even after the end of the DPA.

12. Final Provisions

37. The applicable law is determined by the Principal Agreement.

38. Place of jurisdiction is determined by the Principal Agreement.

39. With the conclusion of this DPA, all previous contracts, if any, concluded between the parties to this contract and which regulate the Processing of the Data on behalf of the Customer are revoked, if and insofar as they relate to the same subject-matter of this DPA and if and insofar as the parties have not expressly agreed otherwise in writing.

40. Amendments and additions to this DPA, as well as the termination of this clause must be made at least in electronic format.

41. Should one or more provisions of this DPA be invalid or unenforceable, this shall not affect the validity of the remaining provisions. Rather, the invalid provisions shall be replaced by way of a supplementary interpretation by such a provision which comes as close as possible to the economic purpose visibly pursued by the parties with the invalid provision(s). If the above-mentioned supplementary interpretation is not possible due to legally binding requirements, the Contracting Parties shall agree on a corresponding provision.

_____

The DPA is concluded in electronic format and is effective without the signatures of the parties.

Date: July 8, 2026.

13. Annex: Subject-Matter of the Processing

The following information on the nature and purposes of the Processing, the nature of the Data and the categories of Data Subjects determine the subject matter of the Processing governed by the DPA. Changes to the subject-matter of the Processing and other procedural changes must be jointly agreed between the Contracting Parties and must be documented.

Purposes of Processing

Personal data of the Customer shall be processed on the basis of this Data Processing Agreement for the following purposes:

42. Support and administration of websites, social media and other communication and information channels.
43. Creation and/or processing of personal profiles.
44. Email marketing.
45. Collection and processing of contact information, addresses and leads.
46. Processing within the framework of AI processes, i.e., using Artificial Intelligence (AI) in accordance with Article 4 of the AI Regulation.
47. Customer management and / or customer support.
48. Software-as-a-Service (SaaS).

Types and Categories of Data

The types and categories of personal data processed on the basis of this DPA include:

49. Master/ Inventory data.
50. Contact information.
51. Content data.
52. Images and/or video recordings.
53. Contract details.
54. Log data.
55. Meta/communication data.

Categories of Data Subjects

The categories of data subjects affected by the processing of personal data on the basis of this DPA include:

56. Website visitors.
57. Software users.
58. Target groups of marketing measures.

Sources of the Processed Data

The data processed on the basis of this DPA are collected or otherwise received from the sources or within the framework of the procedures mentioned below:

59. Collection from data subjects.
60. Inputs or information provided by the Customer.
61. Inputs or information provided by the Processor.
62. Collection in the context of the use of software, websites and other online services.

Appendix: Competent Persons and Contact Persons

Competent persons and contact persons at the Customer:

Carlos León Bolaños
Calle Hermano Pedro, 4
38010 Santa Cruz de Tenerife
España

Physical Access Control

Physical access control measures have been taken to prevent unauthorised persons from physically approaching the systems, data processing equipment or procedures by which the Data are processed.

63. With the exception of the workstation computers and mobile devices, no data processing systems are maintained on the Processor's own business premises. The client's data is stored with external server providers in compliance with the requirements for Processing.
64. Data carriers are stored securely and adequately protected against access by unauthorised persons.

Electronic Access Control

Electronic access control measures have been put in place to ensure that access (i.e. already the possibility of exploitation, use or observation) by unauthorised persons to systems, data processing equipment or procedures is being prevented.

65. All data processing systems are password protected.
66. Passwords are generally not stored in plain text and are only transmitted hashed or encrypted.

Transmission Control

Measures have been taken to control the transmission of the Data to ensure that the Data cannot be read, copied, modified or deleted by unauthorised persons during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

67. Mobile data carriers are encrypted.
68. The transmission and processing of the client's personal data via online offers (websites, apps, etc.) is protected by TLS or equivalent secure encryption.

Ensuring the integrity and availability of data as well as the resilience of processing systems

Measures have been taken to ensure that personal data are protected against accidental destruction or loss and can be quickly restored in an emergency.

69. The Data is stored with external hosting providers. The hosting providers are carefully selected and comply with the state of the art in terms of protection against damage caused by fire, moisture, power failures, disasters, unauthorized access, data backup and patch management as well as facility security.

Annex: Sub-Processors

The Processor shall use the following sub-processors in the Processing of data on behalf of the Client:

ALL-INKL: Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); Service provider: ALL-INKL.COM – Neue Medien Münnich, Inhaber: René Münnich, Hauptstraße 68, 02742 Friedersdorf, Germany; Website: https://all-inkl.com/; Privacy Policy: https://all-inkl.com/datenschutzinformationen/. Data Processing Agreement: Provided by the service provider.

Mailjet: Email distribution and email marketing platform; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Service provider: Alt Moabit 2, 10557 Berlin, Germany; Website: https://www.mailjet.com. Privacy Policy: https://www.mailjet.com/privacy-policy/.

Friendly Captcha: CAPTCHA service that is used to verify whether the data entered within our online services (form submissions) was entered by a human or an automated program. To this end, the service analyzes the behavior of the users of our online services based on various characteristics. This analysis starts automatically as soon as a user submit a online form. Various pieces of information are evaluated for the analysis (IP address, the visitor's dwell time on the website or app, or mouse movements of the user, as well as technical information about the device and browser used by the user); Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); Data Processing Agreement: https://friendlycaptcha.com/legal/; Service provider: Friendly Captcha GmbH, Am Anger 3–5, 82237 Woerthsee, Germany; Website: https://friendlycaptcha.com/. Privacy Policy: https://friendlycaptcha.com/legal/privacy-end-users/.