DATA PROCESSING AGREEMENT

Last update: November 2024

This agreement is attached to and forms an integral part of the Contract in force between Jotelulu, S.L. with registered office at Leganitos 47, 4th Floor, 28013 Madrid (Spain), duly registered in the commercial register of its registered office and with Tax Identification Number ESB65814709, duly represented by David Amorín Iglesias (hereinafter, the PROVIDER or "PROCESSOR") and,

On the other hand, any entity which creates a client account for the purpose of using the Services provided by JOTELULU as defined in the Contract (hereinafter the CLIENT or "CONTROLLER").

Whereas, for the execution of its Services, the PROCESSOR needs to process personal data provided by the CLIENT (hereinafter the "Personal Data").

Whereas, in order to regulate such access, both Parties agree to enter into this DPA, which shall be governed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, (hereinafter, the "GDPR"), its implementing regulations and, in particular, by the following.

CLAUSES

1. Purpose

In accordance with Article 28 of REGULATION (EU) 2016/679 of 27 April 2016 of the European Parliament and of the Council on the Protection of Individuals with regard to the processing of their personal data and on the free movement of such data and Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and guarantee of digital rights, the purpose of this agreement is to define the conditions under which JOTELULU is authorized as a PROCESSOR to process personal data on behalf of the CLIENT in connection with the provision of the Services as set out in the Contract.

In case of any conflict between this agreement and the other documents constituting the Contract, this document shall prevail.

The processing of personal data carried out by the PROCESSOR in its capacity as data controller is out of the scope of this Agreement and is carried out under the conditions described in JOTELULU's "Privacy Policy".

Where this Agreement contain terms defined by Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the "RGPD"), such terms shall have the meaning given to them by the RGPD. Other terms beginning with a capital letter have the meaning defined in the Contract.

2. Processing of personal data

By means of this Data Processing Agreement, the PROCESSOR is authorized to process, on behalf of the CLIENT, the personal data to the extent necessary to provide the services contracted by the CLIENT.

The processing will consist, exclusively, in the personal data processing described in the Contract, notably in any applicable Specific Terms and conditions of Services, and in any other personal data processing agreed in writing between the Parties.

3. Duration of the Agreement

This Agreement shall remain in force for the duration of the provision of the Services. Notwithstanding the foregoing, both Parties agree that the provisions of this Agreement, expressly or by implication intended to continue in effect after the termination or expiration of this Agreement or the Services, shall survive and continue to bind both Parties.

The duty of confidentiality between the Parties shall continue beyond the expiration of this Agreement.

4. Obligations of the PROCESSOR

The PROCESSOR, and all its staff, undertakes to:

a. Use the personal data covered by this Agreement, only for the purpose of the provision of the Specific Terms of Services, excluding any use of personal data for its own purposes or for the purpose of a third party, in particular for commercial, marketing, profiling and datamining purposes.

b. Process personal data only under documented CLIENT's instructions as provided in the Contract or otherwise provided in writing by the CLIENT. If the PROCESSOR considers that any of the instructions infringe the GDPR or any other Union or Member State data protection provisions, it shall inform the CLIENT as promptly as possible.

c. Keep, in writing, a record of all categories of processing activities carried out on behalf of the CLIENT, containing all the mandatory provisions listed in the article 30.2 of the GDPR.

d. Not to communicate data to third parties, except with the authorization of the CLIENT as provided under the Contract, or if such communication is required by applicable law, and to manage in accordance with the article "Management of third-party access requests" below, any request received from a third party in order to receive communication of personal data covered by this agreement. If the PROCESSOR must transfer personal data to a third country or an international organization, pursuant to applicable Union or Member State law, it shall inform the CLIENT of this legal requirement in advance, unless the law prohibits it for important reasons of public interest.

e. Ensure that the persons authorized to process personal data undertake expressly and in writing to respect confidentiality and to comply with the corresponding security measures, of which they must be duly informed.

f. Keep at the disposal of the CLIENT the documentation accrediting compliance with the obligation established in the previous section.

g. Guarantee the necessary training in the protection of personal data of the persons authorized to process personal data.

h. Assist the CLIENT, through appropriate technical and organizational measures, in fulfilling its obligation to respond to requests for exercising the data subject rights laid down in the GDPR in the conditions of the article "Data subject requests management" below.

i. Assist the CLIENT in ensuring compliance with the obligations set out in Articles 33 and 34 of the GDPR taking into account the nature of the processing and the information at its disposal, and notably notify the CLIENT, under the conditions set out in the article "Personal data breaches", of all the personal data breaches that are the subject of this Agreement and which it becomes aware of.

j. Support the CLIENT in carrying out data protection impact assessments where appropriate pursuant to article 35 of the GDPR.

k. Support the CLIENT in carrying out prior consultations with the supervisory authority pursuant to article 36 of the GDPR, where appropriate.

l. Make available to the CLIENT all information necessary to demonstrate compliance with its obligations pursuant to article 28 of the GDPR, as well as for the performance of audits or inspections carried out by the CLIENT or another auditor authorized by the CLIENT. Such audit shall be performed under the conditions of the article "Audit and control" below.

m. Assist the CLIENT in guaranteeing compliance with the obligations set out in Article 32 of the RGPD, implement and maintain the technical and organizational measures described in the document “Infrastructure and Security”, in order to guarantee an appropriate level of security of the personal data subject of this agreement in accordance with said Article 32, and inform the CLIENT of any changes to said measures that may affect the protection of the said data.

n. At the end of the Contract, for whatever reason, return to the CLIENT, on request and under the conditions set out in article 11 “Data portability” below, the personal data covered by this agreement, and delete any copies of said data still in its possession within a period of 60 working days; subject to copies that may be retained on the basis of a legitimate interest or a legal obligation.

5. Obligations of the CONTROLLER

The CLIENT is deemed to be the controller of the processing of personal data subject of this agreement, and undertakes to:

a) In order to permit the provision of the Service, make available to the PROCESSOR all the personal data and/or information necessary for the appropriate operation of the processing activities.

b) Deliver to the PROCESSOR the data referred to in clause II of this document.

c) Carry out an assessment of the impact on the protection of personal data of the processing operations to be carried out by the PROCESSOR.

d) Carry out the appropriate prior consultations.

e) Ensure, prior to and during the processing, compliance with the GDPR by the PROCESSOR.

f) Supervise the processing, including the performance of inspections and audits.

g) Inform the data subjects of the conditions under which their personal data is processed and the conditions for exercising their rights in accordance with the regulations in force.

h) If the CLIENT is not the controller of the processing of personal data covered by the present agreement and/or if there are joint controllers of the said processing, agree with the third party(ies) controller(s), on the conditions of the said processing of personal data, as required by applicable law.

6. Subprocessing

The PROCESSOR has the general authorization from the CLIENT to entrust third parties (hereinafter the "sub-processors") with the processing of Personal Data covered by this agreement.

The existing sub-processors are listed at https://jotelulu.com/en-gb/subprocessors/.

The PROCESSOR shall impose by contract (or by another legal act under the law of the European Union or the law of a member state) to sub-processors, the same obligations with regard to the protection of personal data as those set out in this Agreement, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing meets the requirements of the GDPR.

If the PROCESSOR have recourse to a new sub-processor during the course of the agreement, the PROCESSOR shall notify the CLIENT in writing with reasonable prior notice (if possible at least fifteen (15) calendar days), specifying: (a) the identity of the sub-processor, (b) the processing of personal data that the PROCESSOR intends to entrust to the sub-processor, and (c) the location(s) from which such processing of personal data will be carried out by the sub-processor.

The CLIENT shall notify the PROCESSOR in writing within fifteen (15) days following the sending of the previous notification, of any objection to the intervention of the new sub-processor, specifying the reasons for such an objection. In this case, the Parties shall meet as soon as possible to try to agree on a solution acceptable to each of them. In case of failure to find an acceptable solution, the Services concerned may be terminated by either of the Parties within a reasonable period of time, allowing the CLIENT to ensure the reversibility of the Services.

Sub-processors may be located outside the EU/EEA. If a sub-processor is located in a jurisdiction outside the EU/EEA which is not on the list approved by the European Commission of third countries that ensure an adequate level of protection pursuant to article 45 of the GDPR, appropriate safeguards , such as standard data protection clauses adopted by the Commission pursuant to article 46 of the GDPR, shall be provided by the PROCESSOR and the sub-processor before any data transfer in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermine. The list of sub-processors available on JOTELULU's Website, specify the location of each sub-processor, as well as the appropriate safeguards provided if necessary. Upon CLIENT's request, the PROCESSOR shall provide any useful additional information concerning such safeguards, notably a copy of any applicable standard data protection clauses.

The PROCESSOR shall remain fully liable to the CLIENT for the performance of the obligations of any sub-processor.

7. Security Measures and Personal data breaches

The PROCESSOR shall apply and maintain appropriate technical and organisational measures to protect the personal data it processes on behalf of the CLIENT against unauthorised or unlawful access and processing, and against accidental loss, destruction, damage, theft, alteration, or disclosure, in accordance with the Data Processing Agreement. Such measures are appropriate to ensure a level of security that is adequate to the risk and are adopted considering the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing, as well as varying likelihoods and severities of risks to the rights and freedoms of natural persons. In this regard, The PROCESSOR may update the technical and organisational measures, provided that such modifications do not decrease the overall level of security.

The personal data breaches covered by this agreement and which the PROCESSOR is aware of shall be notified to the CLIENT, without undue delay, and, in any case, within a maximum period of 48 hours.

This notification shall be carried out by sending an e-mail to the address recorded by the CLIENT in its Client account.

The notice shall contain, as a minimum, the following information:

i. Description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records affected.
ii. Name and contact details of the data protection officer or other point of contact from whom further information may be obtained.
iii. Description of the possible consequences of the personal data breach
iv. Description of the measures taken or proposed to be taken by the PROCESSOR to remedy the personal data breach, including, where appropriate, measures taken to mitigate the possible negative effects.

If and to the extent that it is not possible to provide the information simultaneously, the information shall be provided in a phased manner without undue delay.

It is the responsibility of the CLIENT and/or in the case may be of any third-party controller to notify personal data breaches subject of this agreement to the Competent Authorities and to data subjects as soon as possible, where the breach is likely to result in a high risk to the rights and freedoms of natural persons.

8. Responsibilities and guarantees

If the PROCESSOR breaches this Agreement or any Data Protection Law or regulation in determining the purposes and means of processing, it shall be considered

CONTROLLER for such processing, thereby assuming all liabilities, claims and direct penalties that may arise for the CLIENT from such breach by the PROCESSOR.

The PROCESSOR shall only be liable for damage caused by processing in cases where (i) it has not complied with the obligations of the GDPR relating specifically to processors or (ii) it has acted contrary to the CLIENT's lawful written instructions. In such cases, the liability provision of the Contract to which this Agreement is part of shall apply.

In the event that the PROCESSOR and CLIENT engage, as provided in this Agreement, in a processing process that may result in damage to the Data Subject, CLIENT shall, in the first instance, bear the full compensation (or any other compensation) due to the Data Subject and thereafter claim from PROCESSOR the proportionate part of the compensation corresponding to PROCESSOR'S share of liability for such losses, provided that any limitation of liability as provided in the Contract which this Agreement is part of shall apply.

Furthermore, both parties agree that failure to comply with these obligations shall be grounds for termination of this Agreement.

As described on the General Terms and Conditions of Service, PROCESSOR's total cumulative liability will not exceed the services fees paid by the CLIENT during the 12-month period immediately preceding the event giving rise to the claim.

9. Audit and controls

The CLIENT reserves the right to carry out, at its sole discretion, any verification it deems useful to establish compliance by the PROCESSOR with its obligations in relation to the Personal Data processing subject of this agreement. The PROCESSOR undertakes to respond to any audit request by the CLIENT and audit operation carried out by the CLIENT or by a third party chosen by the CLIENT.

On-site audits are carried out at reasonable intervals (no more than once a year), during the PROCESSOR's working days and hours, and must in no way disrupt the PROCESSOR's activities. Audits are carried out at the CLIENT expense and may be invoiced to the CLIENT by the PROCESSOR on the basis of the time spent at reasonable market fee.

The CLIENT shall notify the PROCESSOR in writing, with reasonable prior notice (minimum 30 days), of its wish to carry out an audit, specifying the purpose and scope of the audit and the information to which it wishes to have access to, provided that the purpose and the scope of audit must relate exclusively to the data processing operations covered by this Agreement. In particular, the audit may not relate to the PROCESSOR's financial, accounting or commercial data.

The PROCESSOR undertakes to cooperate and, where appropriate, to ensure that its sub-processors cooperate with the CLIENT in such operations, by providing all relevant information and access to the specific resources used to process the CLIENT's Personal Data. The auditor is not allowed to access resources used by or for other clients of the PROCESSOR, nor resources shared between the CLIENT and other clients of the PROCESSOR. Notably, the CLIENT is not authorized to carry out, or have carried out, penetration testing in the said shared resources (in particular the Website and the Platform), nor physical intrusion tests in the physical site(s) and/or Datacenter(s) used by the PROCESSOR.

At the CLIENT's request, the PROCESSOR must provide a managerial summary of a technical audit report on the above-mentioned shared resources. This audit must be carried out by an independent auditor and be less than three years old. If the CLIENT wishes to carry out intrusion tests on the resources specifically made available to it as part of the Services, a specific agreement must first be signed between the PROCESSOR and the CLIENT, and, where applicable, the third-party auditor(s).

If the audit performed reveals a breach of the warranties and undertakings of the PROCESSOR and, where applicable, of its sub-processors, the PROCESSOR shall take immediate steps to remedy them at its own expense.

If the CLIENT would like to appoint a third-party auditor, the latter must (i) be an auditor recognized for his expertise, (ii) not be a competitor of the SUBCONTRACTOR and (iii) undertake in writing to the PROCESSOR to respect the confidentiality of all documents and information communicated to him or to which he will have access in the course of the audit. The PROCESSOR reserves the right to refuse third-party auditors for just cause (in particular conflict of interest).

If the audit is carried out at the request of the CONTROLLER, the CLIENT shall bear all costs and professional fees arising from the audit, fixed on the basis of the time spent at reasonable market fee.

At the end of the audit, a copy of the entire audit report is communicated to the PROCESSOR as soon as it has been finalized.

10. Data Subject Requests management

The PROCESSOR Assist the CLIENT, through appropriate technical and organizational measures, in fulfilling its obligation to respond to requests for exercising the data subject rights laid down in the GDPR, notably the following rights:

1. Access, rectification, deletion, and opposition.
2. Limitation of processing.

3. Data portability.
4. Not to be subject to automated individualized decisions (including profiling).

In particular, when data subjects send requests for exercising their rights to the PROCESSOR, the latter shall communicate such requests to the CLIENT by e-mail to the contact address provided by the CLIENT in its Client account. The request must be communicated to the CLIENT as soon as possible, and in any event within 7 days of receipt.

In addition, the PROCESSOR undertakes to :

a) Assist the CLIENT in processing the said data subject requests, in particular by providing, on demand, any necessary information in its possession;

b) Ensure the availability of Services in accordance with its contractual commitments, so that the CLIENT is able to deploy solutions and organization appropriate to process data subject requests in accordance with applicable law.

The PROCESSOR should under no circumstances respond, in the name and on behalf of the CLIENT, to requests it receives, except otherwise agreed between the Parties.

11. Data portability

In accordance with the article“Period and End of Services” of the General Terms and Conditions of Service, the CLIENT is responsible for the operations necessary to ensure the portability of personal data covered by this agreement.

JOTELULU undertakes to:

(i) Ensure the availability of the Services and assist the CLIENT, in order to enable the CLIENT, before the effective date of termination or expiry of the Services, to organize and carry out the said portability operations, in particular backup, migration and restoration of the personal data on new infrastructure;

(ii) upon request, and provided that this request is feasible and communicated to the PROCESSOR at least 30 days before the effective date of termination or expiry of the Contract, return to the CLIENT at the end of the Services, whatever the cause, in a readable and usable format, a copy of all the requested data available as part of the Service at the agreed date.

The copies of the data mentioned in point (ii) above may be subjected to reasonable market fee that is systematically provided to the Client for prior approval. The methods for calculating the costs as well as the timeframe for the return of the copy and the return formats, are communicated to the Client upon request to Client Support.

The procedures for moving virtual machines/containers are described on the JOTELULU Portal.

The PROCESSOR communicates its reversibility policy to the CLIENT on request.

12. Management of third-parties access requests

If it receives a request from a third party, including an authority (administrative, judicial, governmental or other), to obtain communication of personal data that is the subject of this Agreement, the PROCESSOR undertakes to:

a) Inform the CLIENT as soon as possible (unless prohibited by applicable European Union regulations),

b) Ask the third party to communicate its request directly to the CLIENT and,

c) In the event of refusal by the third party, systematically oppose the request unless it is established that the request comes from a competent authority acting in execution of a decision recognized and enforceable in application of European Union law and the law of the European Union Member State to which the processing concerned falls in accordance with Article 48 of the RGPD, in which case the communication of data must be exclusively limited to what is required by the decision.

The PROCESSOR undertakes to keep a register of third-party requests for communication of Personal Data that is the subject of this Agreement containing, in particular, a copy of the request and the responses made, the list of data transmitted, the recipient(s) and the dates of communication.

13. Points of contact

For all matters relating to personal data protection, and in particular for all notifications to be made pursuant to this agreement, the Parties agree to use the following contact points:

To contact the CLIENT:

The contact point indicated by the CLIENT in the information linked to its Client Account.

To contact the PROCESSOR:

dpd@jotelulu.com