Data Processing Agreement

pursuant to Art 28 GDPR

(hereinafter referred to as "DPA")

concluded between

Company Name
Address
Company Register Number

(hereinafter "**Controller**")

and

revenue cloud solutions GmbH
Im unteren Angel 1
77652 Offenburg

(hereinafter "**Processor**")

Controller and Processor hereinafter jointly referred to as "**Parties**".

Preamble

The Controller has engaged the Processor to provide certain services and, in this context, has entered into a contract (hereinafter the "Contract"). Part of the performance of the Contract involves the processing of personal data. In particular, Article 28 GDPR imposes certain requirements for such processing on behalf of the Controller. In order to comply with these requirements, the Parties conclude the following DPA, the fulfilment of which shall not be separately remunerated unless expressly agreed.

1. Description of the Processing

The details of the processing activities, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the Controller, are specified in Annex I or arise from the Contract.

2. Obligations of the Parties

2.1. Instructions

a) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Controller may issue further instructions during the entire period of the processing of personal data. All instructions shall be documented at all times.

b) The Processor shall inform the Controller without undue delay if, in its opinion, an instruction infringes Regulation (EU) 2016/679 or applicable data protection laws of the Union or the Member States.

2.2. Purpose Limitation

The Processor shall process the personal data only for the specific purpose(s) set out in Annex I, unless further instructions are given by the Controller.

2.3. Duration of Processing of Personal Data

The data shall only be processed by the Processor for the period specified in Annex I.

2.4. Security of Processing

a) The Processor shall implement at least the technical and organisational measures specified in Annex II to ensure the security of personal data. This includes protection against a personal data breach that, whether accidental or unlawful, leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (hereinafter "personal data breach"). When assessing the appropriate level of security, the Parties shall duly take into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, as well as the risks to the rights and freedoms of data subjects.

b) The Processor shall grant access to personal data undergoing processing only to those members of its personnel who are strictly necessary for the performance, management, and monitoring of the Contract. The Processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

2.5. Special Categories of Data

Where the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health, sex life or sexual orientation of a person, or data relating to criminal convictions and offences (hereinafter referred to as "special categories of personal data"), the Processor shall apply specific restrictions and/or additional safeguards.

2.6. Documentation and Compliance with the Clauses

a) The Parties must be able to demonstrate compliance with these Clauses.
b) The Processor shall handle the Controller's requests regarding data processing under these Clauses promptly and appropriately.
c) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations laid down in these Clauses and directly arising from Regulation (EU) 2016/679. Upon request by the Controller, the Processor shall also allow for and contribute to audits of processing activities covered by these Clauses at reasonable intervals or where there are indications of non-compliance. When deciding on a review or audit, the Controller may consider relevant certifications held by the Processor.
d) The Controller may carry out the audit itself or mandate an independent auditor. Audits may include inspections at the Processor's premises or physical facilities where applicable and shall be carried out, where appropriate, with reasonable advance notice.
e) The Parties shall, upon request, make available to the competent supervisory authority(ies) the information referred to in this Clause, including the results of audits.

2.7. Use of Sub-processors

a) The Processor has the Controller's general authorisation to engage sub-processors, as listed in an agreed list (Annex III). The Processor shall inform the Controller in writing at least one month in advance of any intended changes to this list by adding or replacing sub-processors, thereby allowing the Controller sufficient time to object to such changes before engaging the relevant sub-processor(s). The Processor shall provide the Controller with the information necessary to exercise its right to object.
b) Where the Processor engages a sub-processor to carry out specific processing activities (on behalf of the Controller), this engagement shall be done by way of a contract that imposes on the sub-processor, in substance, the same data protection obligations as those imposed on the Processor under these Clauses. The Processor shall ensure that the sub-processor fulfils the obligations to which the Processor is subject in accordance with these Clauses and Regulation (EU) 2016/679.
c) The Processor shall provide the Controller, upon request, with a copy of such a sub-processing agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the Processor may redact the text of the agreement before providing a copy.
d) The Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations under the contract concluded between the Processor and the sub-processor. The Processor shall notify the Controller if the sub-processor fails to fulfil its contractual obligations.

2.8International Data Transfers

a) Any transfer of data by the Processor to a third country or an international organisation shall only occur on the basis of documented instructions from the Controller, or in order to comply with a specific provision under Union law or the law of a Member State to which the Processor is subject, and must be in full compliance with Chapter V of Regulation (EU) 2016/679.

b) The Controller hereby consents that, in cases where the Processor engages a sub-processor to perform specific processing activities (on behalf of the Controller) and such processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Processor and the sub-processor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the European Commission pursuant to Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the application of such standard contractual clauses are fulfilled.

3. Support for the Controller

a) The Processor shall promptly notify the Controller of any request received from a data subject. The Processor shall not respond to such requests itself unless it has been authorised to do so by the Controller.

b) Taking into account the nature of the processing, the Processor shall assist the Controller in fulfilling the Controller's obligation to respond to requests from data subjects exercising their rights. In fulfilling its obligations under points (a) and (b), the Processor shall act in accordance with the instructions of the Controller.

c) In addition to the obligation of the Processor to assist the Controller pursuant to Clause 3(b), and taking into account the nature of the processing and the information available to the Processor, the Processor shall also assist the Controller in ensuring compliance with the following obligations:

   1. The obligation to carry out a data protection impact assessment (hereinafter "DPIA") where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
   2. The obligation to consult the competent supervisory authority or authorities prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;
   3. The obligation to ensure that personal data are accurate and kept up to date by promptly informing the Controller if the Processor becomes aware that the personal data it processes are inaccurate or outdated;
   4. Obligations under Article 32 of Regulation (EU) 2016/679.

d) The Parties shall specify in Annex II the appropriate technical and organisational measures by which the Processor shall assist the Controller in the implementation of this Clause, as well as the scope and extent of the required assistance.

4. Notification of Personal Data Breaches

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller to enable the Controller to comply with its obligations pursuant to Articles 33 and 34 of Regulation (EU) 2016/679, taking into account the nature of the processing and the information available to the Processor.

4.1. Personal Data Breach relating to Data Processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller as follows:

a) - in the prompt notification of the personal data breach to the competent supervisory authority or authorities after the Controller becomes aware of the breach, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
b) - in gathering the following information, which must be included in the Controller's notification pursuant to Article 33(3) of Regulation (EU) 2016/679, including at a minimum:

   1. • the nature of the personal data, where possible indicating the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
   2. • the likely consequences of the personal data breach;
   3. • the measures taken or proposed by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide all of the above information at the same time, the initial notification shall contain the information available at that time, and further information shall be provided as soon as it becomes available and without undue delay.

c) - in complying with the obligation under Article 34 of Regulation (EU) 2016/679 to notify the data subject of the personal data breach without undue delay where the breach is likely to result in a high risk to the rights and freedoms of natural persons.

4.2. Personal Data Breach relating to Data Processed by the Processor

In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after becoming aware of the breach. Such notification shall at least include:

a) - a description of the nature of the breach (where possible, indicating the categories and approximate number of data subjects concerned and the approximate number of personal data records concerned);
b) - the contact details of a point of contact where more information about the personal data breach can be obtained;
c) - the likely consequences and the measures taken or proposed to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, not all of this information can be provided at the same time, the initial notification shall contain the information available at that time, and further information shall be provided as soon as it becomes available and without undue delay.

The Parties shall specify in Annex III any further information to be provided by the Processor to assist the Controller in complying with its obligations pursuant to Articles 33 and 34 of Regulation (EU) 2016/679.

5. Breaches of the Clauses and Termination of the Contract

a) If the Processor fails to comply with its obligations under these Clauses, the Controller may – without prejudice to Regulation (EU) 2016/679 – instruct the Processor to suspend the processing of personal data until compliance with these Clauses is ensured or the

Contract is terminated. The Processor shall promptly inform the Controller if, for any reason, it is unable to comply with these Clauses.

b) The Controller is entitled to terminate the Contract, insofar as it concerns the processing of personal data pursuant to these Clauses, if:

   1. (a) the Controller has suspended the processing of personal data by the Processor in accordance with this provision and compliance with these Clauses is not reinstated within a reasonable period, but in any event within one month following suspension;
   2. (b) the Processor commits a material or persistent breach of these Clauses or fails to fulfil its obligations under Regulation (EU) 2016/679;
   3. (c) the Processor fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses or Regulation (EU) 2016/679.

c) The Processor is entitled to terminate the Contract, insofar as it concerns the processing of personal data under these Clauses, where the Controller insists on the performance of its instructions which the Processor has notified as being in breach of applicable legal requirements pursuant to Clause 2.1(b).

d) Upon termination of the Contract, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or return all the personal data to the Controller and delete existing copies, unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with these Clauses.

ANNEX I

Description of the Processing

Categories of data subjects whose personal data are processed

- Employees of the customers

Under certain conditions[1]: Guests of the customers

Categories of personal data processed

- Identification data (name, title, position)
- Contact data (email address, telephone number, postal address)
- Technical data (IP address, browser type, activity logs)
- Communication data (email, chat logs, customer interactions)

Under certain conditions[1]: Guest data (name, email address, postal address)

Nature of Processing

The Processor processes booking data and relevant external demand data on behalf of hotels. Using such data and intelligent algorithms, optimisation of pricing and other distribution decisions is performed to increase revenue.

Purpose(s) for which the personal data are processed on behalf of the Controller

The purpose of the processing is

- revenue optimisation ;
- effective pricing;
- maximisingbooking occupancy ; and
- increasing operational efficiency for hotels .

Duration of Processing

The duration of the processing is determined by the contract concluded between the Parties for the provision of the services.

[1] Guest data is collected exclusively under the following conditions: When using certain APIs placeholder systems, guest data is initially transferred and then stored in encrypted form. No further processing takes place; in particular, there is no analysis, profiling or transfer to third parties. Only authorised administrators have access on the basis of a role and authorisation concept.

ANNEX II

Technical and organisational measures, including measures to ensure the security of data

EXPLANATION:

A. Confidentiality

Physical access control: Protection against unauthorised access to data processing facilities by:

Keysystem	

Access control: Preventing unauthorised use of systems:

Passwords	Encryption of storage media
Automatic lock mechanism	Separate user account for each employee
Separation of production and test systems	

Access rights control: preventing unauthorised reading, copying, alteration or removal within systems:

Standard permission profiles on a need-to-know basis	Standard process for granting permissions
Logging of access	Secure storage of storage media
Periodic review of granted permissions, in particular administrative accounts	Data protection-compliant re-use of storage media
Segregation of administrator privileges among multiple persons	

B. Data ingegrity

Transmission control: Preventing unauthorised reading, copying, alteration or removal during electronic transmission or transport:

Encryption of storage media	Encryption of files

Encryption of electronic transmission	

Input control: Ability to verify whether and by whom personal data have been entered, altered or removed from data processing systems:

Logging	Document management

C. Availability and resilience

Availability control: Protection against accidental or intentional destruction or loss through:

Backup strategy (online/offline; on-site/off-site)	Uninterruptible power supply
Anti-malware protection	Firewall
Incident notification channels and contingency plans	Security checks at infrastructure and application level
Standard processes for employee transfers and leavers	

Ability to restore availability and access to personal data in a timely manner:

☒ Yes	☐ No

D. Procedures for regular testing, assessment and evaluation

Regular data protection aduits / monitoring of data protection compliance	Maintaining a record of processing activities
Designation of a Data Protection Officer	Employee confidentiality undertakings
Inventory of all service providers / tools (Vendor Mgmt)	

Data protection management, including regular employee training:

☒ Yes	☐ No

Policies implemented under the data protection management system:

Internal data protection Policy	Password Policy
Third-party / vendor management Policy	Data retention and deletion Policy
Handling data subject rights	Handling personal data breaches
Clean desk Policy	Bring your own device (BYOD) Policy
Remote Work Policy	Social Media Policy
Acceptable Use Policy	

Incident-Response-Management:

☒ Yes	☐ No

Processor control: Ensuring that processing on behalf of the controller is carried out only on documented instructions within the meaning of Art. 28 GDPR:

Clear contractual arrangements	Careful selection of the processor (e.g. ISO certification)

Annex III

List of Sub-processors

Explanation:

List of sub-processors that are deemed approved at the time of signing the data processing agreement between the processor and the controller.

Company	Address	Service	Third-country-transfer
MongoDB, Inc.	New York, Paramount Plaza, 1633 Broadway, 38th Floor, United States	Database services	Adequacy decision (Art. 45 GDPR); EU-US DPF certified
Amazon Web Services EMEA Sàrl	38 Avenue John F. Kennedy, L-1855, Luxembourg	Hosting - services	n/a
Twilio Inc. (Sendgrid)	101 Spear Street, First Floor, San Francisco, CA 94105, United States	Email delivery services	Adequacy decision (Art. 45 GDPR); EU-US DPF certified