Data Processing Agreement

This Data Processing Agreement is applicable to all processing of personal data to be undertaken by Redforts Software S.L., registered with the Madrid Chamber of Commerce (Registro Mercantil de Madrid) under fiscal number ES-B85946390, (hereinafter: Processor) for the benefit of another party to whom it provides services (hereinafter: Controller).

This Data Processing Agreement was last amended on 7 May 2018.

1. Purposes of processing

1.1. Processor hereby agrees under the terms of this Data Processing Agreement to process personal data on behalf of the Controller. Processing shall be done solely for the purpose of the contracted service Oscar Hotel Software (hereinafter: Oscar), and all purposes compatible therewith or as determined jointly.

1.2. The personal data to be processed by Processor for the purposes as set out in the previous clause and the categories of data subjects involved are set out in Appendix 1 to this Data Processing Agreement. Processor shall not process the personal data for any other purpose unless with Controller's consent. Controller shall inform Processor of any processing purposes to the extent not already mentioned in this Data Processing Agreement.

1.3. All personal data processed on behalf of Controller shall remain the property of Controller and/or the data subjects in question.

2. Processor's obligations

2.1. Regarding the processing operations referred to in the previous clause, Processor shall comply with all applicable legislation, including all applicable data processing legislation such as the General Data Protection Regulation (GDPR).

2.2. Upon first request Processor shall inform Controller about any measures taken to comply with its obligations under this Data Processing Agreement.

2.3. All obligations for Processor under this Data Processing Agreement shall apply equally to any person processing personal data under the supervision of Processor, including but not limited to employees in the broadest sense of the term.

2.4. Processor shall inform Controller without delay if in its opinion an instruction of Controller would violate the legislation referred to in the first clause of this article.

2.5. Processor shall provide reasonable assistance to Controller in the context of any privacy impact assessments to be made by Controller, in case this is required by law. Processor can charge reasonable costs for doing so.

3. Transfer of personal data

3.1. Processor may process the personal data in any country within the European Union.

3.2. Transfer to countries outside the European Union is also permitted, provided that the legal requirements for doing so have been fulfilled.

3.3. Processor shall report to Controller of the countries involved outside the EU.

4. Allocation of responsibilities

4.1. Processor shall make available IT facilities to be used by Controller for the purposes mentioned above.

4.2. Processor is solely responsible for the processing of personal data under this Data Processing Agreement in accordance with the instructions of Controller and under the explicit supervision of Controller. For any other processing of personal data, including but not limited to any collection of personal data by Controller, processing for purposes not reported to Processor, processing by third parties and/or for other purposes, the Processor does not accept any responsibility.

4.3. Controller declares and warrants that the content, usage and instructions to process the personal data as meant in this Data Processing Agreement are lawful and do not violate any right of any third party. Controller shall indemnify the Processor for any claims which are the result of non-compliance of Controller with applicable privacy legislation and/or this Data Processing Agreement.

5. Involvement of sub-processors

5.1. The Controller hereby grants permission to the Processor, within the framework of the Processor's Agreement, to engage third parties. The Processor shall inform the Controller about any proposed changes in third parties engaged. The Controller has the right to object (in writing, within two weeks and supported by arguments) to a proposed new/changed third party. Should the Controller object, the Parties will jointly endeavour to find a solution.

5.2. In any event, Processor shall ensure that any third parties are bound to at least the same obligations as agreed between Controller and Processor. Controller has the right to inspect the agreements containing such obligations.

5.3. Processor declares and warrants that these third parties shall comply with the obligations under this Data Processing Agreement and is liable for any damages caused by violations by these third parties as if it committed the violation itself.

6. Security

6.1. Processor shall use reasonable efforts to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the processing operations involved, against loss or unlawful processing (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed).

6.2. Processor has implemented the security measures as per Appendix 2. Processor does not warrant that the security is effective under all circumstances.

6.3. Controller shall only provide personal data to Processor for processing if it has ensured that the required security measures have been taken. Controller is responsible for the parties' compliance with these security measures.

7. Notification and communication of data breaches

7.1. Controller is responsible at all times for notification of any security breaches and/or personal data breaches (which are understood as: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed) to the competent supervisory authority, and for communication of the same to data subjects. In order to enable Controller to comply with this legal requirement, Processor shall notify Controller within 48 hours after becoming aware of an actual or threatened security or personal data breach.

7.2. A notification under the previous clause shall be made at all times, but only for actual breaches.

7.3. The notification shall include at least the fact that a breach has occurred. In addition, the notification shall:

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

8. Processing requests from data subjects

8.1. In the event a data subject makes a request to exercise his or her legal rights under data protection legislation to the Processor, the Processor shall pass on such request to Controller, and Controller shall process the request. Processor may inform the data subject of this passing on. The Processor will provide assistance with handling a request, to the extent necessary and reasonable. The Processor can charge reasonable costs for such assistance.

9. Confidentiality obligations

9.1. All personal data that Processor receives from Controller and/or collects itself is subject to strict obligations of confidentiality towards third parties. Processor shall not use this personal data for any goals other than for which it was obtained, not even if the personal data has been converted into a form that is no longer related to an identified or identifiable natural person.

9.2. The confidentiality obligation shall not apply to the extent Controller has granted explicit permission to provide the personal data to third parties, the provision to third parties is reasonably necessary considering the nature of the assignment to Controller or the provision is legally required.

10. Audit

10.1. Controller has the right to have audits performed on Processor by an independent third party bound by confidentiality obligations to verify compliance with the security requirements, compliance with data processing regulations, unauthorised use of personal data by Processor personnel, compliance with the Data Processing Agreement, and all issues reasonably connected thereto.

10.2. This audit may be performed once every year, no earlier than two weeks after the Controller has provided written notice to the Processor.

10.3. Processor shall give its full cooperation to the audit and shall make available employees and all reasonably relevant information, including supporting data such as system logs.

10.4. The audit findings shall be assessed by the parties in joint consultation and may or may not be implemented by either party or jointly.

10.5. The costs of the audit shall be borne by Controller.

11. Liability and contractual fine

11.1. The liability of Processor for any damages as a result of a failure to comply with this Data Processing Agreement, unlawful acts or otherwise, is excluded. To the extent such liability cannot be excluded, it is limited to direct damages per event (a sequence of successive events counting as one event), up to the amount received by Processor for all activities under this Data Processing Agreement for the month prior to the event. Any liability of Processor for direct damages shall in any event never be more than the amount to be paid by the insurer of Processor in such event.

11.2. Direct damages shall include only:

- damages to physical objects;
- reasonable and proven costs to cause Processor to regain compliance with this Data Processing Agreement;
- reasonable costs to assess the cause and extent of the direct damage as meant in this article; and
- reasonable and proven costs that Controller has incurred to limit the direct damages as meant in this article.

11.3. Any liability for indirect damages by Processor is excluded. Indirect damages are all damages that are not direct damages, and thus including but not limited to consequential damages, lost profits, missed savings, reductions in goodwill, standstill damages, failure to meet marketing requirements, damages as a result of using data prescribed by Controller, or loss, corruption or destruction of data.

11.4. No limitation of liability shall exist if and to the extent the damages are a result of intentional misconduct or gross negligence on the part of Processor or its directors.

11.5. Unless Processor is permanently unable to perform an obligation under this Data Processing Agreement, any liability shall exist only if Controller puts Processor on notice of default, including a reasonable term for addressing the failure, and Processor fails to comply even after this term. The notice shall contain a detailed description of the failure to ensure that Processor has a reasonable opportunity to address the failure.

11.6. Any claim for damages from Controller to Processor that is not specifically notified in detail shall be extinguished by the passage of twelve (12) months after the date its cause first arose.

12. Term and termination

12.1. This Data Processing Agreement enters into force upon acceptance by the Controller.

12.2. This Data Processing Agreement is entered into for the duration of the cooperation between the parties.

12.3. Upon termination of the Data Processing Agreement, regardless of reason or manner, Processor shall - at the choice of Controller - return in original format and/or destroy all personal data available to him.

12.4. Processor is entitled to amend this Data Processing Agreement from time to time. Processor shall notify the Controller of amendments at least three months prior to their taking effect. Controller may terminate if the amendments are unacceptable to it.

13. Applicable law and competent venue

13.1. This Data Processing Agreement and its execution are subject to Dutch law.

13.2. To the extent not otherwise provided for in mandatory law, all disputes related to the Agreement will be submitted to the competent court in Utrecht, the Netherlands.

Appendix 1. Stipulation of personal data and data subjects

Personal Data

Processor shall process the below personal data under the supervision of Controller, as specified in article 1 of the Data Processing Agreement:

- Names
- Addresses
- Telephone numbers
- E-mail addresses
- Web sites
- Date of birth
- Place and country of birth
- Language
- Nationality
- Gender
- Tax number
- Occupation
- ID card or passport: number, issuing country, issue date, expiry date
- Credit card details
- Details of arrival and departure
- Booked accommodations
- Used travel agency

Data Subjects

Of the following categories of data subjects:

- Customers of the Controller

- Leads and potential customers of the Controller

Controller declares and warrants that the description of personal data and categories of data subjects in this Appendix 1 is complete and accurate, and shall indemnify and hold harmless Processor for all faults and claims that may arise from a violation of this representation and warranty.

Appendix 2. Implemented security measures

Processor is amongst others PCI-DSS compliant meaning it implemented:

- *Secure network and systems*: Firewall configurations protect the data.
- *Network segmentation*: No direct Internet access to data storage (DMZ).
- *Logical access control*: Access requires asymmetrical key pairs protected by strong passwords.
- *Encrypted transmission*: All data sent over the Internet is encrypted using TLS.
- *Audit trail and logging*: All user actions are logged.
- *Physical access control*: Physical access is controlled and monitored.
- *Organisational measures*: Access to data is limited and defined by need to know.

Signed by Redforts Software S.L.
on 2025-03-25 with a certificate
issued by AC Firmaprofesional -
CUALIFICADOS