Data Processing Agreement

This Data Processing Agreement (DPA) forms an integral part of the services agreement between Oaky and Client (the Agreement). Client (as defined in the Agreement) and Oaky (as defined in the Agreement) have agreed to the following terms in relation to the Processing of Personal Data subject to the Agreement.

This DPA is effective as of the date Client agreed to the Agreement

WHEREAS:

A. Client requests that the Services be supplied as described in and on the terms of the Agreement and Oaky agrees to provide the Services as described in the Agreement.

B. Oaky is a technology partner that helps the Client to provide upsell and cross-sell technology and communication to their guests.

C. As between Client and Oaky, Client is the Data Controller of Personal Data that will be Processed by Oaky as Data Processor on behalf of Client for the purpose of provision of the Services.

D. Client will transfer to Oaky and/or Oaky will collect the relevant Personal Data in respect of C. above.

NOW THEREFORE THE PARTIES AGREE AS FOLLOWS:

1. Definitions & interpretation

1.1 In the event of conflict or inconsistency between this DPA and any of the terms and conditions of the Agreement, including any in respect of data protection, this DPA will be given precedence, unless otherwise set out herein.

1.2 In this DPA, unless otherwise defined, all capitalised words and expressions shall have the following meaning:

(a) **Client Personal Data** means any Personal Data Processed by Oaky on behalf of Client to or in connection with the Agreement and this DPA.

(b) **Data Protection Law** means local data protection legislation or any statutory equivalent in force in any part of the world which is relevant to Personal Data, including the GDPR.

(c) **EEA** means European Economic Area.

(d) **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

(e) **Integration Partner** means a third party involved by the Client to provide integration services to Client and who acts as a separate data processor on behalf of Client.

(f) **Standard Contractual Clauses** means the Commission Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR (2021/914).

(g) **Security Breach** means any unauthorized or accidental access to, or collection, loss, destruction, damage, or alteration of Client Personal Data, including those resulting from an actual or attempted breach of security measures used to secure Client Personal Data and/or any other irregularity in processing the Client Personal Data.

(h) **Services** means the services provided by Oaky to Client as further detailed in the Agreement.

(i) **Sub-Processor** means a person or entity subcontracted by Oaky to Process Client Personal Data.

The terms **Data Controller, Data Processor, Data Subject, Personal Data, Processing, Supervisory Authority** shall have the meaning given to them in the GDPR.

2. Processing Client Personal Data

2.1 For purposes of this DPA, Oaky is the Data Processor of Client Personal Data and Client is the Data Controller. Annex 1 contains details about the Processing of Client Personal Data by Oaky.

2.2 Oaky shall:

(a) only Process Client Personal Data on behalf of and for the benefit of Client, in accordance with the terms of this DPA together with Client's instructions, unless required to do so by applicable law to which Oaky is subject;

(b) inform Client if, in its opinion, an instruction received from Client infringes Data Protection Law; and

(c) notify Client in the event that it is unable to comply with this DPA or its obligations under Data Protection Law or if it has reason to believe that the legislation applicable to it is likely to have a substantial adverse effect on the obligations provided under this DPA or otherwise prevents it from fulfilling the instructions received from Client under this DPA.

2.3 Client acknowledges and agrees that, for the performance of the Services, Oaky needs to receive Client Personal Data from and share Client Personal Data with Integration Partners upon the Client's and/or the Integration Partner's request thereto. Any sharing of Client Personal Data between Oaky and any Integration Partner falls under the scope of Client's instructions under this DPA. Client acknowledges and agrees that Oaky has no direct contractual relationship with any Integration Partner and that Oaky is not responsible or liable for any modification, damage or deletion of Client Personal Data by an Integration Partner or any other third party with whom Client Personal Data is shared in accordance with this clause 2.3.

2.4 Client shall comply with its respective obligations under Data Protection Law.

3. Rights and obligations of Oaky

3.1 Oaky shall:

(a) keep Client Personal Data confidential and take appropriate technical and organisational security measures, as further specified in Annex 3, to protect Client Personal Data against unauthorised or unlawful Processing, accidental loss or damage or destruction;

(b) only grant access to Client Personal Data to persons under Oaky's authority who are bound by a confidentiality obligation on a need to know basis; and

(c) provide reasonable cooperation and assistance to Client, at the costs and request of the Client, as may reasonably be required to allow Client to comply with its obligations under Data Protection Law, including in relation to data security, data breach notifications, data protection impact assessments, prior consultation with Supervisory Authorities, the fulfilment of data subjects' rights, and an enquiry, notice or investigation by a Supervisory Authority.

4. Security Breaches

4.1 Oaky shall without undue delay inform Client of any actual or suspected Security Breach involving Client Personal Data. Oaky shall, in its reasonable discretion, take adequate remedial measures and shall provide Client with all relevant information and assistance as requested by Client regarding the actual or suspected Security Breach. The notification of a Security Breach to Client will include:

(a) a description of the Security Breach, including the date and time the Security Breach was discovered;

(b) an overview of the affected Client Personal Data and the categories and numbers of affected Data Subjects;

(c) information on the (expected) consequences of the Security Breach; and

(d) a description of the measures taken by Oaky to limit the consequences of the Security Breach.

5. Sub-Processors

5.1 Client hereby grants Oaky general written authorisation for the engagement of Sub-Processors, under the conditions that Processor shall remain fully liable to Client as regard the fulfilment of the obligations of the Sub-Processor and that Oaky and the Sub-Processor have entered into an agreement that imposes obligations on the Sub-Processor that are no less restrictive than those imposed on Oaky under this DPA.

5.2 Oaky shall inform Client of any new Sub-Processors engaged by Oaky. Within 30 days of receiving such notice, the Client may object to such Sub-Processors by providing written notice to Oaky alleging objective justifiable grounds related to the inability of such Sub-Processor to protect Client Personal Data. In the event that the Parties cannot reach a mutually acceptable solution, Oaky shall, at its option, refrain from allowing the Sub-Processor to access the Client Personal Data, or enable the Client to terminate the relevant Services in accordance with the terms of the Agreement.

5.3 The Sub-Processors listed in Annex 3 are hereby approved by Client.

6. Audit Rights

6.1 Oaky shall make available to Client all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client. during normal working days and normal working hours, subject to notice given in advance with a reasonable notice period. Client is responsible for all costs and expenses in relation to the audits.

7. Data transfers

7.1 Oaky will abide by the requirements under Data Protection Law regarding the transfer of Client Personal Data from the EEA to countries outside the EEA. For the purpose of providing the Services under the Agreement, Client Personal Data may be transferred to countries outside the EEA, provided that the transfer is covered by one of the following measures:

(a) an adequacy decision of the European Commission determining that an adequate level of data protection is provided pursuant to Article 45 GDPR;

(b) binding corporate rules approved by a competent Supervisory Authority in accordance with Article 47 GDPR;

(c) an approved code of conduct or certification mechanism pursuant to Article 46 GDPR;

(d) entering into the relevant version of the Standard Contractual Clauses with the recipient of the Client Personal Data pursuant to Article 46 GDPR.

7.2 To the extent that Client is established in a country outside the EEA and the transfer of Client Personal Data from Oaky to Client is not covered by one or more safeguards listed in clause 7.1(a), 7.1(b) or 7.1(c) of this DPA, Parties hereby agree to enter into the Standard Contractual Clauses separately. In the event of a contradiction between this DPA and the provisions of the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail in so far as they are applicable between Parties.

To the extent that a Sub-Processor is based in a country outside the EEA, and the transfer of Client Personal Data is not covered by one or more safeguards listed in 7.1(a), 7.1(b) or 7.1(c) of this DPA, Client authorises Oaky to engage such Sub-Processor, under the condition that Oaky enters into the Standard Contractual Clauses with the Sub-Processor prior to the transfer taking place.

7.3 Client shall provide all reasonable assistance to Oaky and/or any Sub-Processor in relation to the performance of any required transfer impact assessment.

8. Termination and erasure and return of data

8.1 On termination of the Agreement, or earlier as requested by Client, Oaky will destroy, or at Client's election will return to Client, all Client Personal Data in its possession, except for such information as must be retained under applicable law.

8.2 To the extent that Oaky retains any such Client Personal Data beyond termination or expiration of the Agreement or as earlier requested by Client, because such retention is required under applicable law, this DPA will remain in full effect and Oaky will destroy all such Client Personal Data so retained once such retention is no longer required under applicable laws.

8.3 At such time when Client Personal Data is either returned or destroyed in full, this DPA will expire automatically.

9. Liability

9.1 The provisions on (the limitation of liability) of the Parties under the Agreement apply to each Party's liability for breach of this DPA.

10. Applicable law and forum

10.1 This DPA and any dispute or claim arising out of it or in connection with it, its subject matter or formation shall be governed by and construed in accordance with the laws of the Netherlands.

10.2 Any dispute, controversy or claim arising out of or in connection with this DPA, its subject matter or formation shall be submitted to the exclusive jurisdiction of the competent courts of Amsterdam, the Netherlands.

ANNEX 1

Details of processing activities

Subject matter of the processing	Oaky provides Client with upsell and cross-sell services, as further defined in the Agreement between Client and Oaky.
Duration of the Processing	Duration of the Services, as defined in the Terms of Service – Oaky
Purpose and nature of the processing	Providing Services as defined in the Agreement between Client and Oaky.
Types of Personal Data	Customers personal data: - *Name - *Email address - *Telephone number - *Reservation code - **Birthday * Provided by all Clients. ** Only provided by some Clients.
Types of Special Categories of Personal Data (if applicable)	None.
Categories of data subject	Customers of the Client (data controller).
Data Transfers and safeguards (if applicable)	To Integration Partners and Sub-Processor(s). Where these parties are located outside the EEA, Oaky will ensure that (i) their country provides an adequate level of protection in accordance with art. 45 GDPR; or (ii) other appropriate safeguards are in place to ensure an adequate level of protection with respect to privacy rights of individuals as required by Article 46 of the GDPR.

ANNEX 2

Technical and organisational measures

Oaky has implemented the following technical and organisational measures to protect the Client Personal Data:

A. Control environment

a. New employees receive the Oaky Information Security handbook & Code of Conduct and sign off on adhering to it.

b. New employees sign the Oaky NDA as Appendix of their employment contract.

c. Employees receive periodical training on specific subjects (safe working environment, GDPR compliance, etc.).

d. The organization holds bi-yearly risk assessment meetings with the board and management to discuss the current risk analysis, and identify new risks.

e. The organization has considered the potential for fraud in its risk assessment.

f. The organization provides and communicates policies and procedures to its employees.

g. The organization monitors system components through Sentry and Amazon CloudWatch.

B. Logical and physical access controls

a. The organization uses two-factor authentication for access to their applications.

b. Access to infrastructure is managed through the use of a firewall.

c. The organization grants and revokes access to new and previous employees as part of their onboarding and offboarding process. Access is granted based on job profiles.

d. The organization performs quarterly checks on users and the systems they have access to ensure that all employees have appropriate access rights.

e. Physical access to the organizations' office locations is restricted to employees.

f. Physical access to facilities and protected information assets is outsourced to Amazon.

g. Penetration test is carried out annually by a third party.

h. The organization has documented the secure transmission of data for its integrations and implemented measures in conformance with the specifications.

i. Users are not able to deactivate or bypass security settings.

j. Full disk software encryption is enabled on the workstation operating system drives.

k. Critical security updates released by the operating system developer are checked quarterly and installed as soon as possible.

l. Prevent unauthorised persons from gaining access to data processing systems with which personal data are processes or used;

i. Two-factor authentication in place for server management

ii. IP restricted access

iii. Certificate restricted access

m. Prevent data processing systems from being used without authorisation;

i. All systems need valid credentials

n. Ensure that persons entitled to use a data processing system have access only to the Client Personal Data to which they have a right of access;

i. Data access is limited by identification and role management, only authorised users get access to data they are authorised for.

o. Ensure that personal data is adequately protected during transmission or transport;

i. All traffic runs over SSL connections

p. Policy: no connection to unknown Wi-Fi networks

C. System operations

a. The organization has a structured development process in place, supported by a workflow in Jira. Review steps and testing are mandatory.

b. An incident response plan is being followed when an incident takes place.

D. Risk mitigation

a. The organization documents knowledge to ensure that it is retained when staff leave.

b. The organizations' systems are cloud- based, making it possible to work remotely, IT staff use secure VPN connections to access the environment. Access to public wi-fi is not allowed.

c. The organization tests remote access on a weekly basis.

E. Additional security measures

a. Backups and disaster recovery handled by Amazon in a restricted environment

b. Recovery tests are performed on a yearly basis.

c. The organization has data processing agreements with customers and sub service providers in place that limit the use of personal information to the purposes identified in the entity's objectives related to privacy.

d. Procedure in place to comply with the provisions regarding the exercise of rights by the data subject in accordance to Arts. 15, 16, 17, 18, 20, 21 and 22 GDPR

F. Completed Audits

a. Completed SOC2 audit for implementing organisation wide safeguards around data privacy and security. Please let us know if you would like to review the SOC2 report.

ANNEX 3

Approved Sub-Processors

Sub-Processor	City/Country	Service
Amazon Web Services	Germany, Frankfurt	Secure Cloud Service Platform for Database Storage
The Rocket Science Group LLC d/b/a MailChimp	Atlanta, USA	Secure Email Service Platform
Google LLC	Mountain View, USA	Secure Email Data Import Platform only used by Clients that send Client Personal Data via Email to Oaky.
Intercom	Delaware, USA	Chat platform used by Clients to communicate with Oaky Customer Success Team.
Slack	San Francisco, USA	Internal chat platform which may be used to share Client Personal Data among relevant Oaky employees to support an Oaky Client.
Atlassian	San Francisco, USA	Internal notes/ticketing system which may be used to share Client Personal Data among relevant Oaky employees to support an Oaky Client.
Hubspot	Cambridge, Massachusetts, United States	Internal CRM which may be used to share Client Personal Data among relevant Oaky employees to support an Oaky Client.
Sciant AD	Sofia, Bulgaria	Secure, Cloud-Based Service that connects Oaky to other hospitality systems, only used by Clients that use the connectivity supported by Sciant.
SalesForce	Frankfurt, Germany / Paris, France	Internal CRM which may be used to share Client Personal Data among relevant Oaky employees to support an Oaky Client.