Data Processing Agreement in accordance with Article 28 of the General Data Protection Regulation (GDPR)

1. Subject matter and duration of the Agreement

1. This Data Processing Agreement (the "Agreement") governs the processing of personal data processed by the Supplier in the course of providing its services for the Client under a separate agreement (the "Main Agreement"). The subject matter of the Main Agreement is the commissioning of the Supplier with the provision of the SaaS application and the associated smartphone app (“platform”). In the context of this engagement, it is necessary for the Supplier to process personal data for which the Client is the data controller within the meaning of the EU General Data Protection Regulation ("GDPR").
2. This contract is attached to the general terms and conditions of the Supplier as **Annex III** and shall be deemed to be an integral part thereof.
3. From a data protection perspective, the processing activities in question qualify as processing on behalf of the Client within the meaning of Article 4 (2) and Article 28 of the GDPR, and therefore, the Supplier assumes the role of data processor from a data protection perspective. The Supplier declares that it is capable of carrying out the commissioned services in accordance with Article 28 of the GDPR.
4. This Agreement governs the data protection measures within the meaning of Article 28 GDPR as well as the rights and obligations of the Client and the Supplier to fulfil data protection requirements.
5. The Agreement shall enter into force upon signing the Main Agreement. The duration of the Agreement and termination options are governed by the Main Agreement.

2. Categories of data processed, and data subjects concerned

1. The categories of data processed, and the categories of data subjects concerned by the processing are listed in **Annex 1**.
2. No special categories of personal data within the meaning of Article 9 (1) of the GDPR are processed.

3. Obligations of the Supplier

3.1. General Information

1. The Supplier collects, stores and processes personal data on behalf of and according to the instructions of the Client. The Client remains data controller in terms of data protection law.
2. The Supplier is not entitled to use data for its own purposes or to transmit it to third parties without consent of the Client given in text form.
3. The Supplier shall process personal data within the scope of the Agreement exclusively within the European Union/the European Economic Area, unless stipulated otherwise in **Annex 3**. This does not apply if the Client is located in a third country outside the EU/EEA. For this purpose, standard contractual clauses within the meaning of Article 46 (2) c of the GDPR shall be concluded (see **Annex 4**).

3.2. The Supplier is bound to instructions

1. The Supplier undertakes to process data and processing results exclusively within the framework of the provisions of this Agreement and based on documented instructions of the Client. Copies or duplicates of the data shall not be created without Client's knowledge, except for necessary backup copies to ensure proper data processing and data required to comply with statutory retention obligations.

2. Instructions are generally agreed upon in the Main Agreement. Further or subsequent instructions may be issued by the Client in documented form, including text form and electronic form (e.g., by email without electronic signature). The Supplier shall promptly confirm verbal instructions in text form.
3. The Supplier shall promptly inform the Client if it believes that an instruction of the Client violates data protection provisions of the European Union or its member states. It is the responsibility of the Client to correct its instruction if necessary. The Supplier has the right to suspend the implementation of the instruction until it has been modified by the controller to comply with the law.
4. If the Supplier receives a governmental request to disclose data of the Client, the Supplier shall - to the extent permitted by law – promptly inform the Client and refer the authority to the Client. The Client and Supplier shall cooperate with the supervisory authority upon.

3.3. Documentation obligation

1. The Supplier shall keep a record of processing activities in accordance with Article 30 (2) of the GDPR.
2. Changes to the subject matter of the processing shall be jointly agreed upon with the Client and set out in text form.

3.4. Confidentiality

1. The Supplier is obliged to maintain data secrecy in addition to specific legal confidentiality obligations.
2. The Supplier ensures that all individuals entrusted with data processing have been obliged to maintain confidentiality prior to commencing their duties or that they are subject to an appropriate statutory obligation of confidentiality.
3. The confidentiality obligation of the individuals engaged in data processing remains in effect even after their activities have ended and they have left the Supplier’s organization.

3.5. Technical and organizational measures

1. The Supplier guarantees the security and therefore confidentiality, integrity and availability of the data in accordance with Article 32 of the GDPR. In this sense, the Supplier has taken all necessary technical and organizational measures to ensure the security of the processing pursuant to Art 32 et seq of the GDPR. These measures specifically include data security measures and measures to ensure an appropriate level of protection in terms of confidentiality, integrity, availability and the resilience of the systems. Details regarding these measures can be found in **Annex 2** (Technical and organizational measures). The Supplier confirms that, in implementing these measures, it has taken into account the state of the art, the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR. The Supplier assures that the measures pursuant to **Annex 2** ensure a level of security appropriate to the risks associated with the processing and the nature of the data to be protected.
2. The technical and organizational measures are subject to technical progress and further development. The Supplier is permitted to implement alternative adequate measures provided that the level of security of the specified measures is not compromised. Any significant changes shall be documented.

3.6. Data subject rights

1. The Client is solely responsible and competent for safeguarding data subject rights. The Supplier may only implement data subject rights upon the instruction of the Client. However, the Supplier shall assist the Client in the fulfilment of requests and claims of data subjects.
2. The Supplier shall take the necessary technical and organizational measures to ensure that the Client can fulfil the data subject rights in accordance with Chapter III of the GDPR (information, access, correction and deletion, data portability, objection, as well as automated decision-making in individual cases) at any time within the statutory timeframes. The Supplier shall support the Client in fulfilling its obligation to respond to data subjects' requests and promptly provide the Client with all necessary information upon request. This

also includes support in fulfilling the rights to restriction of processing, as well as the obligation to notify in connection with the rectification or erasure of personal data or the restriction of processing.

3. The Supplier shall support the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR. This includes implementing data security measures, reporting personal data breaches to the supervisory authority, notifying affected individuals of personal data breaches, conducting data protection impact assessments, and engaging in prior consultation.
4. Requests from data subjects regarding their rights or requests for information, corrections or deletions shall be promptly forwarded by the Supplier to the Client for processing. Information to third parties may only be provided in accordance with the Client's instructions or shall be forwarded to the Client for processing. Likewise, information may not be provided directly to employees of the Client, but only via the agreed contact person.
5. The Supplier may not independently correct, delete or restrict the processing of data processed under the Agreement, but only in accordance with documented instructions from the Client. If a relevant request is addressed to the Supplier and if the Supplier indicates that the requester mistakenly considers the Supplier to be controller for the data application, the Supplier shall promptly forward the request to the Client and inform the requester accordingly. The Client shall designate a contact person responsible for data protection for such purpose.
6. If the Supplier becomes aware of violations of the protection of personal data of the Client, the Supplier shall inform the Client without undue delay and take the necessary measures to secure the data and to mitigate any possible adverse consequences of the data subjects.
7. The Supplier shall notify the Client without undue delay - but no later than 24 hours after becoming aware of it - of any malfunctions, infringements by the Supplier or its employees, as well as any breaches of data protection regulations or the provisions established in the Agreement, and any suspicion of data protection breaches or irregularities in the processing of personal data. This shall also apply in particular with regard to any reporting and notification obligations of the Client pursuant to Article 33 and 34 of the GDPR. The Supplier warrants that it will, if necessary, provide the Client with appropriate support in fulfilling its obligations under Articles 33 and 34 of the GDPR (see Article 28 (3) Sentence 2 (f) of the GDPR). The Supplier may only carry out reports under Articles 33 or 34 GDPR on behalf of the Client upon prior instruction.

3.7. Rights of inspection and control

1. With regard to the processing of data provided by the Client, the Client is granted the right to inspect and control the data processing facilities at any time, including by third parties commissioned by the Client. The Supplier undertakes to provide the Client with the information necessary to monitor compliance with the obligations set out in this Agreement.
2. The Supplier shall allow pre-announced inspections during business hours by an independent third party. Such inspections shall be carried out in a manner that does not disrupt the Contractor's business operations. The costs incurred by such inspections shall be shared between the Client and the Contractor or agreed on a case-by-case basis. Should a case of hardship arise that requires an inspection without prior notification, the costs shall be borne in full by the Client. The Contractor shall be entitled to reasonable remuneration for all services in connection with the support of inspections.
3. In cases where the Client is subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claims of a data subject or a third party or any other claim related to the data processing carried out by the Supplier, the Supplier shall provide the Client with its best efforts to support.

4. Subcontracts

1. Subcontracts within the scope of this provision refers to services directly related to the provision of the main service. It does not include ancillary services that the Supplier may use, such as telecommunication services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Supplier is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Client's data also in the case of outsourced ancillary services.
2. The Supplier is authorized to engage subcontractors (sub-processors) for the performance of the Service. The subcontractors engaged at the time of concluding this Agreement are listed in **Annex 3**. The planned engagement shall be notified to the Client in text form with reasonable advance notice. The Client may object to the planned engagement. If the Client does not raise any objection within 30 days, the assignment shall be deemed approved.
3. In the event of an objection being raised in accordance with Section 4.2, the Supplier shall be entitled to terminate the Agreement with immediate effect in text form or in writing by registered letter to hotelkit GmbH, Marie-Andeßner-Platz 1, 5020 Salzburg or by e-mail to info@hotelkit.net.
4. When engaging a subcontractor, the Supplier must conclude a data processing agreement with the subcontractor in accordance with Article 28 (4) of the GDPR. In doing so, it must be ensured that the subcontractor undertakes the same obligations as those imposed on the Supplier under this Agreement.
5. If the subcontractor fails to comply with its data protection obligations, the Supplier shall be liable to the Client for the subcontractor's compliance with those obligations.

5. Liability

1. The liability of both parties is defined in the General Terms and Conditions for the Main Agreement.
2. Notwithstanding the above, the Client shall be liable to the Supplier for the legality of all instructions issued and shall indemnify and hold the Supplier harmless from and against any and all damages and disadvantages resulting from compliance with an instruction.

6. Procedure after completion of processing services

1. After completion of the processing, at the latest after termination of the contract, the Contractor shall hand over to the Client all documents and processing or usage results that have come into its possession or personal or other confidential data produced or copied for the fulfillment of the service in connection with the contractual relationship and/or destroy or securely delete them in accordance with data protection regulations in consultation with the Client. This obligation shall also apply to the same extent to any subcontractors engaged. Data whose deletion is not possible for technical reasons or would involve a disproportionately high effort, as well as copies that are necessary to prove the correctness of data processing or to fulfill liability and warranty claims, remain unaffected. Personal data must always be deleted; if this is not possible, it must be anonymized.
2. For such data, processing shall be restricted in accordance with Article 18 of the GDPR. Data may be retained by the Supplier in accordance with the respective retention periods beyond the end of the Agreement and must be securely deleted upon expiration of the retention periods. The Client shall be informed about the type and scope of the stored data. The Supplier may transfer this data to the Client at the end of the Agreement as evidence of compliance.
3. After the termination of the Agreement, the Supplier provides written confirmation to the data controller regarding the secure deletion or destruction of all documents in its possession.

7. Contact person

As for the Supplier, the following contact persons are named:

Person authorized to receive instructions at the Supplier:
Marius Donhauser, Managing Partner
Email Address: marius.donhauser@hotelkit.net

Contact person regarding Data Protection:
Eric Schicht, Data Privacy Officer & Quality Manager
Email Address: dataprivacy@hotelkit.net

The Client shall provide the Supplier with a person authorized to give instructions and a contact person for data protection as part of the onboarding process.

8. Final provisions

1. Exclusive place of jurisdiction is 5020 Salzburg, Austria. To the extent permissible under mandatory law, Austrian law shall apply exclusively, to the exclusion of the conflict-of-law rules of the Austrian Private International Law Act (IPRG) and the UN Convention on Contracts for the International Sale of Goods (Federal Law Gazette 1988/96).
2. Any existing data protection agreements of the contracting parties will be mutually terminated upon the entry into force of this Agreement.
3. If any provision of this Agreement is or becomes invalid or unenforceable, either in whole or in part, it will not affect the validity or enforceability of the remaining provisions. The invalid or unenforceable provision shall be replaced by a valid or enforceable provision that reflects the economic intent of the original provision to the greatest extent possible. This same principle will apply to any gaps or omissions in this Agreement.
4. Any amendments and supplements to this Agreement must be made in text form. This text form requirement can only be waived by agreement in text form. No verbal agreements exist as additional terms to this Agreement.
5. In the event of changes in the legal circumstances that affect the validity of this Agreement, the parties undertake to collaborate towards legally effective modifications to this Agreement.
6. **Annexes 1 to 3** form an integral part of the Agreement. If amended, they shall be attached to the Agreement and shall replace the corresponding old Annex in the Agreement.
7. **Annex 4** only applies if the Client has its registered office in a third country as defined in Article 44 of the GDPR.

Annex 1: Types of data processed, and affected people

The categories of data subjects affected by the processing include:

- Client (see Client Data),
- Employees of the Client and other employee-like persons authorized by the client to use the platform (see Employee Data),
- Vendors of the Client (see Vendors Data),
- Customers of the Client ("**Customer/s**") and other persons in the client's facilities and other affected parties (see Customer Data).

The following categories of personal data are processed by the Supplier within the context of the data processing agreement:

Part A: General Data

This part covers all personal data that can be processed across divisions within the network. There is no technical obligation to enter data, unless otherwise stated. However, the Client may require that the data be recorded within the framework of operational agreements.

Employee Data

Designation	Description	Purpose of Use
Name	First name and surname of the data subject	Clear identification of the user in the communication within the Client's circle of employees
E-mail address[1]	Work email address of the employee	- Delivering notifications - Reset access data - Newsletter (consent required)
Gender	Gender of the employee	Gender-specific wording
Position[1]	Position in the company	Internal communication, representation for clear role assignment
Phone number[1]	Work phone number of the employee	Internal communication
Birthday[1]	Birthday of the employee	Internal communication
Department[1]	Department where the employee works	Internal communication, representation for clear role assignment
Hiring date[1]	Date of entry into operation	Internal communication
Photograph[1]	Photo of the employee or profile picture	Internal communication, easy identification
Correspondence data, translation data	Data in connection with the provision of the work owed by employees, data on guest inquiries, data from internal chats and notes as well as data in translated texts.[3]	Internal communication including Google translate.
Text data, content data	Content, comments, correspondence, handbook articles written by the data subject.	Internal communication
Photos and files	Photos and files uploaded by the data subject.	Internal communication

Client Data

Designation	Description	Purpose of Use
Name[2]	First name and surname of data subject	Provision (storage) of customer information
Contact information[2]	Deposited contact data, address, email, phone number	Provision (storage) of customer information

Vendor Data

Designation	Description	Purpose of Use
Name[2]	First name and surname of the data subject	Provision (storage) of vendor information
Contact information[2]	Deposited contact data, address, email, phone number, belonging to company	Provision (storage) of vendor information

Customer Data

Bezeichnung	Beschreibung	Verwendungszweck
Name[2]	First name and surname of the data subject.	Provision (storage) of customer information
Contact information[2]	Stored contact details, address, e-mail, telephone number.	Provision (storage) of customer information
Information about the stay[2]	Information on the duration of the stay.	Provision (storage) of customer information
Nationality[2]	Nationality of Customer.	Provision (storage) of customer information
Sex[2]	Sex of Customer.	Provision (storage) of customer information
Information on inquiries and incidents[2]	Correspondence data and data on inquiries and incidents in connection with Customers.	Communication and Provision (storage) of customer information.
Data on translations[3]	All categories of data translated using Google Translate, in particular data relating to inquiries from Customers or data from internal notes and data in translated texts.[3]	Communication including Google Translate and Provision (storage) of customer information.
Photos and files[2]	Photos and files uploaded by the data subject.	Provision (storage) of customer information

Footnotes:

[1]optional, as far as deposited by the respective user

[2]optional, if this information is saved by the Client in the platform

[3] In addition, service data is generated when using Google Translate (see Google's privacy policy).

Part B: Technical data

This part covers personal data generated by the data subject through activity within the network. All data is collected by the data subject themselves.

These data concern all of the above categories of data subjects.

Designation	Description	Purpose of Use
Activity	Name of the activity carried out	- Internal communication - Traceability of activities
Creation time	Time at which the activity was carried out or content was created	- Technically necessary - For the traceability of activities
Time of reading access	Time at which an employee accessed new content for the first time	- Technically necessary for information about changes - Traceability of the acknowledgement
IP address	IP address of the connection from which the access is made	Ensuring data security, technically necessary
Transmitted data	Amount of data transmitted	Ensuring data security
Browser and device version	Browser and devices used	Data security, provision of functionalities depending on compatibility
Model	When using iOS or Android app: Model name	For the provision of functions depending on the compatibility with the device
Last login	Last active login on the platform	Ensuring data security

Additional technical data regarding app use

Designation	Description	Purpose of Use
Session device data	Device name, device manufacturer, location, session time	Security function: Display of registered devices

Annex 2: Technical & organizational measures

1. Physical access control

Unauthorized access is to be prevented, with the term being understood to be spatially.
Technical or organizational measures for access control, in particular also for the authentication of authorized persons:

- To prevent physical access to the Client's data, security personnel are permanently located in the Supplier's data centers. The areas are also under video surveillance in all areas.

2. Data access control

Technical (password protection) and organizational (user master record) measures regarding user identification and authentication:

- Only authorized technicians with the appropriate individual user rights have access to the servers. Secure access connections (via encrypted VPN tunnel) and authentication control technologies (authentication via username and password) are implemented to regulate access to the systems and internal support.

3. Authorization control

Unauthorized activities in IT systems outside of granted authorizations must be prevented.
Demand-oriented design of the authorization concept and the access rights as well as their monitoring and logging:

- The client determines through user settings and rights management in the software who has access to which information. The Client establishes guidelines for the length, complexity and expiration of passwords.
- The aforementioned access controls secure access to the personal data collected as part of the services.
- Access is restricted to employees of the contractor with corresponding responsibilities through an authorization concept. The number of Supplier's employees with authorizations is reduced to the "bare minimum”.

4. Transfer control

Aspects of the transferring personal data need to be regulated, including electronic transfer, data transfer, data transport, transmission control, etc.
Measures for transport, transmission and transfer or storage on data carriers (manual or electronical) as well as during subsequent verification:

- Data transmission occurs via the HTTPS protocol. By utilizing up-to-date encryption based on TLS (Transport Layer Security), the Supplier ensures the highest possible level of data protection during transmission.

5. Input control

Ensuring traceability and documentation of data management and maintenance. Measures for subsequent verification of data input, modification, or removal (deletion) and identification of the responsible party:
Access to or modification of the personal data transmitted is subject to effective access protection mechanisms as described under item 3 above.

- Input, modifications, and deletions of data are logged through session logs.

6. Processing control

Ensuring compliant data processing in accordance with instructions.
Measures (technical/organizational) for defining the responsibilities between the Client and the Supplier:

- The software and system architecture allow for the implementation of instructions from the client regarding the input, modification, or removal of personal data.
- The selection of subcontractors by the Supplier has been conducted with careful consideration, particularly regarding data security.
- Control rights over the Supplier have been defined.
- The Supplier's employees are bound by confidentiality obligations.
- Data destruction after the completion of the assignment is ensured.

7. Availability control

The data shall be protected against accidental destruction or loss.
Measures for data security (physical / logical):

- By distributing the systems across different data centers, very high availability can be achieved and maintenance work on the infrastructure can be carried out without affecting accessibility.
- All changes are captured in hourly backups. Weekly backups also provide further security against data loss and enable a stable and fast recovery of databases and files.
- All software used is regularly updated to the latest version. This way, possible security gaps in all areas are eliminated as quickly as possible.
- The use of antivirus programs and a firewall prevents the occurrence of malicious code.
- Monitoring all resources enables preventive intervention and serves to detect problems and possible attacks at an early stage. This can ensure that smooth and secure access is possible.
- The selected data centers have an excellent internet connectivity. The direct connection of the subcontractors mentioned in the attachment enables fast and stable access worldwide. Here, too, a high level of availability can be guaranteed with various routes, even in the event of disruptions outside the data center.
- Reporting channels are defined and known to the employees.
- Emergency plans for rapid recovery are in place and regularly reviewed for effectiveness.

8. Separation control

Data collected for different purposes shall also be processed separately.
Measures for separate processing (storage, modification, deletion, transmission) of data with different purposes:

- Processing and backups are always stored on several storage media in spatially separated areas to ensure separation.
- Data records are labelled with purpose attributes.
- Clear database rights are defined.
- Logical software-based separation by tenants is implemented.
- Separate development, testing, and production systems ensure distinct separation of the used data.

9. Pseudonymization

Processing data in a way that does not allow the identification of specific individuals without additional information from a separate source:

- Pseudonymization through the use of unique identification numbers (ID).

- Separate storage of the mapping between IDs and specific individuals.

10. Further measures

To meet the specific requirements of data protection, adjustments and internal measures have been implemented:

- Development of a privacy and IT security concept.
- Regular training for employees.
- Implementation of a data protection management system with processes for regular review, assessment and evaluation of the effectiveness of measures taken.
- Privacy-friendly default settings.

Annex 3: Sub-processors

Sub-processor Infrastructure - Data Storage			
Company name	Address	Service provided	Measures for an adequate level of data protection
hotelkit technik UG	hotelkit technik UG (haftungsbeschr.), Teplitzer Str. 34, D-01219 Dresden, Germany	• Development of the platform • Support of the server and network infrastructure of hotelkit GmbH	Data Processing Agreement
1&1 IONOS SE	1&1 IONOS SE, Elgendorfer Str. 57, D-56410 Montabaur	• Bereitstellung Virtual Server für Live-Umgebung • Data Location: Karlsruhe	Data Processing Agreement
diva-e Datacenters GmbH	diva-e Datacenters GmbH, Kruppstraße 105, D-60388 Frankfurt/Main	• Bereitstellung Dedicated Server für Live-Umgebung • Data Standort: Frankfurt	Data Processing Agreement
ANEXIA Internetdienstleistungs GmbH	Anexia Deutschland GmbH, Hofmühlgasse 3, A-1060 Wien	• Provision of virtual server for reverse proxy server • Data Location: Wien	Data Processing Agreement
Hetzner Online GmbH	Hetzner Online GmbH, Industriestr. 25, D-91710 Gunzenhausen	• Provision of dedicated servers for storing encrypted backups • Data Location: Falkenstein in Sachsen	Data Processing Agreement

Sub-processors Service-specific			
Company name	Address	Service provided	Measures for an adequate level of data protection
Microsoft Corporation	Walter-Gropius-Straße 5, 80807, München, Germany	• SMTP relay management	Data Processing Agreement The EU Commission has issued an adequacy decision for this third country, which you can access here. Microsoft Corporation is certified under the EU-U.S. Data Privacy Framework on which the EU Commission's adequacy decision is based. You can request the certification here.
salesforce.com Germany GmbH	Erika-Mann-Str. 31, 80636, München, Germany	• CRM and lead management	Data Processing Agreement
Atlassian, Public limited company	Level 6, 341 George Street, NSW 2000, Sydney, Australia	• Administration and forwarding of support requests	Data Processing Agreement andStandard Contractual Clauses for the transfer of personal data to a third country
Google Cloud EMEA Limited* * for users in Austria. The Google company responsible in other countries can be found at the following link:	70 Sir John Rogerson's Quay, Dublin 2, Irland	• Automatic translation of texts entered by the author (use of multiple languages) by Google Translate	Data Processing Agreement

https://cloud.google.com/terms/google-entity.			
Celonis, Inc.	Theresienstr. 6,80333, Munich, Germany	• CRM and Leadmanagement • Automation	Data Processing Agreement
PandaDoc, Inc.	3739 Balboa Street. Suite #1083, San Francisco, CA 94121, USA	• Quotation and contract preparation and administration • Creating e-signatures	Data Processing Agreement The EU Commission has issued an adequacy decision for this third country, which you can access here. PandaDoc, Inc. is certified under the EU-U.S. Data Privacy Framework on which the EU Commission's adequacy decision is based. You can request the certification here.
HubSpot, Inc.	25 First Street, Cambridge, MA 02141 USA	• CRM and marketing management	Data Processing Agreement The EU Commission has issued an adequacy decision for this third country, which you can access here. HubSport, Inc. is certified under the EU-U.S. Data Privacy Framework on which the EU Commission's adequacy decision is based. You can request the certification here.

Annex 4: Standard contractual clauses

STANDARD CONTRACTUAL CLAUSES

(MODULE FOUR: Transfer processor to controller)

SECTION I

Clause 1

Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

b) The Parties:

I. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

II. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   I. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   II. Clause 8.1(b), 8.9(a), (c), (d) and (e)
   III. 9(a), (c), (d) and (e)
   IV. Clause 12(a), (d) and (f);
   V. Clause 13;
   VI. Clause 15.1(c), (d) and (e);
   VII. Clause 16(e);
   VIII. Clause 18(a) and (b)

b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay - but no later than 24 hours - after becoming aware of it and assist the data importer in addressing the breach.

c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

Not applicable.

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

e) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

Not applicable.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   I. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   II. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (*As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.*);

   III. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

I. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

II. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes

that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   I. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within 30 days of suspension;

   II. the data importer is in substantial or persistent breach of these Clauses; or

   III. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal

data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Austria.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Austria.

B. LIST OF PARTIES

Data exporter(s):

Name of the data exporter(s)	***Address of the data exporter(s)***	***Contact details of the contact person***	***Activities relevant to the data transferred under these Clauses***	***Role***	***Where applicable, data exporter's data protection officer***
hotelkit GmbH	Altes Mühlhaus, Marie-Andeßner-Platz 1, 5020 Salzburg, Austria	Name: Marius Donhauser Position: CEO E-mail: marius.donhauser@hotelkit.net	See Annex 1	Processor	Name: Eric Schicht E-mail: dataprivacy@hotelkit.net

Data importer(s):

Name of the data importer(s)	***Address of the data importer(s)***	***Contact details of the contact person***	***Activities relevant to the data transferred under these Clauses***	***Role***	***Accession date and signature***	***Where applicable, data importer's data protection officer***
See main contract.	See main contract	See main contract	See main contract	Controller	See main contract	See main contract

C. DESCRIPTION OF TRANSFER

Purpose of the data processing:

☒ The processor processes personal data on behalf of the controller for the purposes of providing the services defined in the Main Agreement

☐ Other:

Nature of the data processing activities performed by processor under the Contract:

☒ Collection or recording of personal data

☒ Organization or structuring of personal data

☒ Storage of personal data

☒ Adaptation or alteration of personal data

☒ Retrieval or consultation of personal data

☐ Use of personal data

☒ Disclosure of personal data by transmission, dissemination or otherwise making available

☐ Alignment or combination of personal data

☒ Restriction of personal data

☒ Erasure or destruction of personal data

☐ Other:

Categories of data subjects:

See Annex 1 of the Data Processing Agreement.

Type of personal data:

See Annex 1 of the Data Processing Agreement.

Duration of the data processing:

☒ The duration of the data processing is the same as the duration of the Main Agreement

☐ Other:

The frequency of the transfer:

☐The data is transferred on a one-off

☒ Continuous basis

☐ Other: