Data Processing Agreement of the Internet-Based Hotel Management Software

This Data Processing Agreement is Appendix 3 to the contract for the use of the internet-based hotel management software of HotelFriend Service GmbH between HotelFriend ("Contractor") and the customer ("Client"). Unless otherwise defined in this contract, the terms used herein have the meaning given to them in the contract for the use of the internet-based hotel management software of HotelFriend Service GmbH. The terms and definitions of Regulation (EU) 2016/679 (hereafter "GDPR"), particularly Art. 4 GDPR, also apply to this Data Processing Agreement.

1. Subject of the Contract

1.1 The subject of this Data Processing Agreement is to define the data protection framework for the contractual relations between the parties.

1.2 The subject of the order results from the software contract, which is referred to here (hereinafter referred to as "Service Agreement") as well as from the contracts yet to be concluded.

2. Support and Services

2.1 The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area.

2.2 Any transfer of processing to a third country requires the prior consent of the Client in written form and may only occur if the specific conditions for transfer to a third country under Art. 44 and following of the GDPR are met.

3. Duration

3.1 The duration of this order corresponds to the term of the Service Agreement.

3.2 The Client can terminate this contract without notice if there is a serious breach by the Contractor of data protection regulations or the provisions of this contract. In particular, non-compliance with the obligations agreed in this contract and derived from Art. 28 GDPR constitutes a severe breach.

4. Scope, Type & Purpose of Data Processing (Art. 4 No. 2 GDPR)

4.1 Processing is necessary for the performance of a contract or pre-contractual measures in accordance with Art. 6 Para. 1 lit. b GDPR. The processing is also necessary to protect the legitimate interests of the data controller or a third party in accordance with Art. 6 Para. 1 lit. f GDPR.

4.2 The subject of the processing of personal data includes the following types/categories of data:

4.2.1 Personal master data (name, address, possible date of birth)

4.2.2 Contact details of the employees and service providers of the client who are affected

4.2.3 Communication data (e.g., telephone, email)

4.2.4 Contract master data (contractual relationship, order status information, product or contractual interests)

4.2.5 Customer history (data from offers, order confirmations and invoices)

4.2.6 Contract accounting and payment data (bank, payment and account information data, tax-relevant data)

4.2.7 Planning and control data

5. Categories of Affected Individuals

The following groups of the Client's affected individuals are subject to processing:

5.1 Existing customers and interested parties in the products and/or services

5.2 Employees, as well as external service providers of the Client, who are commissioned with the fulfillment of the above mentioned processing purposes

5.3 Trade representatives and other contacts on the part of the client and contractor who are involved in the fulfillment of the above mentioned processing purposes

5.4 Tax consultants

6. Instructions

6.1 The Contractor processes personal data only within the scope of instructions issued by the Client. This does not apply insofar as the Contractor is obliged to process under the law of the EU or the Member States to which the Contractor is subject. In this case, the Contractor informs of these legal requirements before processing, unless such notification is prohibited by the relevant law due to an important public interest.

6.2 Regardless of the form of issuing, both the Contractor and the Client shall document each instruction of the Client in text form. The instructions are to be kept for the duration of this contract and another three years thereafter.

6.3 The Contractor shall immediately inform the Client if, in their opinion, an instruction issued by the Client violates statutory provisions. In such a case, the Contractor is entitled, after timely prior notice to the Client, to suspend the execution of the instruction until the Client has changed or confirmed it. If the Contractor can demonstrate that processing per the Client's instruction could lead to the Contractor's liability under Article 82 of the GDPR, the Contractor reserves the right to suspend further processing until the issue of liability has been clarified between the parties.

6.4 The Client determines the person or persons authorized to issue instructions. The Contractor identifies the recipient of instructions. In the event of a change or longer-term prevention of the contact persons, the

successor or representative must be immediately informed in written or electronic form to the contractual partner.

7. Contractor's Support Obligations

7.1 Given the nature of the processing, the Contractor takes appropriate technical and organizational measures to assist the Client in fulfilling his duty to respond to requests from data subjects under Articles 12 to 22 of the GDPR.

7.2 Considering the nature of the processing and the information available to him, the Contractor assists the Data Controller in complying with his obligations under Articles 32 to 36 of the GDPR. Specifically, in the security of processing, in reporting violations to the supervisory authority, in notifying affected persons of a violation, in the data protection impact assessment, and in consulting the competent supervisory authority.

7.3 If a data subject or a data protection supervisory authority directly contacts the Contractor in relation to the personal data processed under this Agreement, the Contractor shall promptly inform the Client and coordinate further steps with him.

8. Client's Audit Rights

8.1 The Contractor shall provide the Client, upon request, with all necessary information to verify compliance with the obligations stipulated in this contract and Article 28 of the GDPR. In particular, the Contractor shall provide the Client with information about the stored data and data processing programs.

8.2 The Client or third parties appointed by the Client are—usually subject to making an appointment—entitled to check compliance with the obligations from this contract and from Article 28 of the GDPR and to carry out on-site inspections at the Contractor's premises. The Contractor facilitates this and contributes to it.

8.3 The Contractor is obligated to provide the Client, upon request, with suitable evidence of compliance with the obligations as per Article 28, Paragraph 1 and 4 of the GDPR. This evidence can be provided by submitting documents and certificates that represent approved codes of conduct in accordance with Article 40 of the GDPR, or approved certification procedures in accordance with Article 42 of the GDPR.

9. Notification of Contractor's Violations

9.1 The Contractor assists the Client in complying with the duties referred to in Articles 32 to 36 of the GDPR concerning the security of personal data, notification duties in the event of data breaches, data protection impact assessments, and prior consultations. Among others, these include:

9.1.1 Ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing, the projected probability and severity of a possible legal violation due to security gaps, and allow for instant identification of relevant violation events

9.1.2 Obligation to immediately report any violations of personal data to the Client

9.1.3 Obligation to support the Client in fulfilling his duty to provide information to the data subject and to immediately provide him with all relevant information in this context

9.1.4 The support of the Client in his data protection impact assessment

9.1.5 Supporting the Client in the context of prior consultations with the supervisory authority

9.2 The Contractor may claim compensation for support services that are not included in the service description or that are not attributable to the Contractor's misconduct.

10. Quality Assurance and Other Obligations of the Contractor

10.1 In addition to complying with the provisions of this contract, the Contractor has legal obligations under Articles 28 to 33 of the GDPR; in this respect he especially guarantees compliance with the following requirements:

10.1.1 Preservation of confidentiality as per Art. 28 Para. 3 Sentence 2 lit. b, 29, 32 Para. 4 GDPR. The Contractor employs only staff members in the execution of the work who have been committed to confidentiality and previously familiarized with the data protection provisions relevant to them. The Contractor and every person under his authority who has access to personal data may only process this data as instructed by the Client, including the powers granted in this contract, unless they are legally required to do the processing.

10.1.2 Implementation and adherence to all necessary technical and organizational measures for this order as per Art. 28 Para. 3 Sentence 2 lit. c, 32 GDPR [details in Chapter 13].

10.1.3 The Client and the Contractor, on request, cooperate with the supervisory authority in compliance with its tasks.

10.1.4 Immediate notification of the Client regarding inspections and actions of the supervisory authority, insofar as they relate to this contract. The same applies if a competent authority carries out investigations with the Contractor in the course of an administrative offense or criminal procedure concerning the processing of personal data in contract processing.

10.2 If the Client is subject to an inspection by the supervisory authority, an administrative offense or criminal procedure, the liability claim of a data subject or third party, or any other claim in connection with the contract processing at the Contractor, the Contractor shall assist the Client to the best of his abilities. The Contractor may charge for support services that are not

included in the service description or are not attributable to misconduct by the Contractor.

10.3 The Contractor regularly reviews the internal processes as well as the technical and organizational measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

10.4 The Contractor ensures the demonstrability of the implemented technical and organizational measures to the client as part of his control powers.

11. Data Protection Officer

11.1 The Contractor ensures the provision of a Data Protection Officer / Contact Person / Representative via the written appointment of a Data Protection Officer who carries out his duties in accordance with Articles 38 and 39 of the GDPR. The contact details will be communicated to the Client for the purpose of direct contact. A change in the Data Protection Officer will be promptly reported to the Client.

11.2 The Contractor's Data Protection Officer is: Mr. Dr. Wilfried Röder, E-mail: datenschutz@infai.org

12. Confidentiality

12.1 The Contractor confirms that he is aware of the data protection regulations pertinent to the order processing under the GDPR. He preserves the data secrecy and confidentiality when processing the personal data of the Client. This obligation continues even after the termination of this contractual relationship.

12.2 The Contractor assures that he will familiarize the employees involved in the execution of the work with the regulations of data protection pertinent to them. He obliges these employees through a written agreement to maintain confidentiality for the duration of their activity and beyond the termination of their employment relationship, unless they are subject to an appropriate statutory obligation of secrecy. The Contractor monitors compliance with data protection regulations in his company.

12.3 The Contractor may only provide information to third parties or those affected with the prior written consent of the Client, or consent in an electronic format.

13. Technical and Organizational Measures

13.1 The Contractor shall document the implementation of the technical and organizational measures outlined and required before the order was placed prior to the start of the processing, particularly with regard to the specific order execution, and submit it to the Client for review. Upon acceptance by the Client, the documented measures become the basis of the contract. If an inspection or audit by the Client reveals a need for adjustment, this is to be implemented by mutual agreement.

13.2 The Contractor is responsible for ensuring security according to Art. 28 Para. 3 lit. c, 32 GDPR, especially in connection with Art. 5 Para. 1, Para. 2 GDPR. Overall, the measures to be taken involve data security measures and ensuring a protection level appropriate to the risk in terms of confidentiality, integrity, availability, and resilience of the systems. The state of the art, the implementation costs, and 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 according to Art. 32 Para. 1 GDPR, must be taken into account.

13.3 The technical and organizational measures are subject to technical progression and further development. The Contractor is therefore allowed to implement alternative suitable measures. However, the security level of the defined measures must not be undershot. Significant changes must be documented.

13.4 Documentation of technical and organizational measures according to Art. 32 GDPR

13.4.1 At HotelFriend Service GmbH, the technical and organizational measures described below are taken to ensure the protection and security of personal data and the right to privacy of the persons concerned.

13.4.2 These measures are regularly reviewed and continuously updated within the framework of the data protection concept. In designing these measures, the statutory protection objectives - confidentiality, integrity and availability of systems and services – were comprehensively taken into consideration, so that an appropriate action plan could be developed.

13.4.3 All processing processes are essentially based on the requirements of Articles 24, 25 and 32 GDPR. This also allows the potential risk associated with handling personal data to be effectively contained in the long term, considering the resilience of the systems, with regard to the type, extent, circumstances, and purpose of the data processing activities.

13.5 Confidentiality (Art. 32 para. 1 lit. b GDPR)

13.5.1 Access and entrance control

13.5.1.1 Technical measures: Fences, gates and other spatial boundaries; securing of windows and doors; Secure VPN connection; Encryption of data carriers and mobile devices, firewall, file servers; Front-end and application systems, and antivirus software are used, if applicable; Logging of access rights; Authentication via password input or biometric scans; Central locking plan with documentation of the keys issued.

13.5.1.2 Organizational measures: Visitor management; key regulations; password rules, including specifications for password complexity (policy); Reliable staff for security and cleaning areas; Creation of user profiles; Assignment of user rights; Role and authorization concept; Control of

maintenance, repair, and cleaning staff; Employees are instructed according to GDPR; Employees are instructed to lock windows and doors outside office hours; Employees are required to activate the automatic desktop lock; All employees are instructed on the clean-desk policy; There is a formal user registration and deregistration for all information systems and services to grant and revoke access permissions.

13.5.2 Access control

13.5.2.1 Technical measures: GDPR-compliant destruction of data carriers, encryption of data carriers and mobile devices; Identification and authentication system (two-factor authentication); Secure storage of data carriers; GDPR-compliant destruction of data carriers; Encryption of data carriers and mobile devices.

13.5.2.2 Organizational measures: Password rules (policy, central password assignment); Authorization concepts; Adjustment to the number of administrators with full access permissions; Authentication with a user profile, password, or certificate is required to access data processing systems; A personal user administration is carried out for all systems worth protecting; Access permissions and profiles are created in a differentiated and task-based manner. The management of user rights is carried out by administrators; There is a regulation with consequences to be initiated in case of the loss of IDs and keys; The IT operations department maintains a record of access using logs of changes and deletions relating to data, timestamps of processing and users; Paper files (if any) are on-site destroyed using a shredder of DIN security level 3. There is a clear instruction for disposal or reuse of devices equipped with storage media; The verification of access rights is continuously carried out by the system administrator.

13.6 Integrity (Art. 32 para. 1 GDPR)

13.6.1 Input control

13.6.1.1 Technical measures: Digital authorization concept; Electronic signature; Email encryption.

13.6.1.2 Organizational measures: Setting up and using individual usernames; Granting of access permissions; Rights for entering, modifying, and deleting data are granted based on an authorization concept.

13.6.2 Separation control

13.6.2.1 Technical measures: Clear separation of data stored for different purposes; The systems for the test and production environment are separate; if applicable, data records are provided with purpose attributes; All personal data is assigned an individual customer number. A logical separation is ensured.

13.6.2.2 Organizational measures: Client separation; Control via authorization concept; Visitor management (here: guest access); The target of the separation requirement is ensured by restrictive access and order control; Private use of company devices is prohibited in writing for all employees.

13.6.3 Dissemination control

13.6.3.1 Technical measures: Digital authorization concept; Secure VPN technology; Email encryption; The IT operations department ensures restricted, encrypted data transmission possibilities; Remote data transmission is encrypted.

13.6.3.2 Organizational measures: Regulations and instructions for data destruction and deletion exist; Granting of access permissions; Archived documents are stored in a locked archive with limited access permissions; Upon departure or transfer of an employee, no longer needed access permissions are revoked or access to IT systems is blocked; Service providers are committed in writing to maintain data secrecy. There are no service providers who have unauthorized access to the office premises.

13.7 Availability and resilience (Art. 32 para. 1 GDPR)

13.7.1 Technical measures: Fire and smoke detectors, fire extinguishers, alarm system; Firewall; Emergency management; Virus protection; All IT systems are redundantly available.

13.7.2 Organizational measures: A backup & recovery concept exists; Documents and data carriers, whose legal, contractual or statutory retention period has expired, are destroyed (deletion concept); Load tests of the systems are carried out as needed.

13.8 Pseudonymization and encryption (Art. 32 para. 1 lit. a GDPR)

13.8.1 Technical measures: External access to the corporate LAN is exclusively via VPN; Access to systems is always encrypted (TLS, SSL); Data transmission on the website is encrypted (TLS, SSL); Electronic communication occurs using SSL/TSL encryption.

13.8.2 Organizational measures: Internal instruction to anonymize or pseudonymize personal data, if possible, in case of transfer or after the legal deletion period has expired; There is an independent WLAN guest access; The individual details that can lift anonymity are stored separately from the other data. Depending on the linkability and the client, the personal reference is restored, if applicable; There are internal instructions to anonymize or pseudonymize personal data, if possible, in case of transfer or after the legal deletion period has expired - if applicable.

13.9 Procedures for regular testing, assessment, and evaluation (Art. 32 para. 1 GDPR; Art. 25 para. 1 GDPR)

13.9.1 Contract conformity / order control

13.9.1.1 A written agreement for processing operations according to Art. 28 of the GDPR is concluded, each

defining the rights and obligations of the contractor and client.

13.9.1.2 There is a prior examination of the security measures taken by the contractor and their documentation.

13.9.1.3 There are contractually established regulations for the use of further subcontractors.

13.9.1.4 There are contractually established responsibilities.

13.9.1.5 Assurance of data destruction after termination of the contract.

13.9.1.6 If the collaboration is of a longer duration: Ongoing review of the contractor and his level of protection.

13.9.1.7 All employees are committed to data secrecy and regularly receive training and instructions on data protection and data security. Data protection training takes place at least every 2 years.

13.9.2 Data protection management

13.9.2.1 A data protection officer has been appointed in writing.

13.9.2.2 The record of processing activities is complete and up-to-date.

13.9.2.3 Service providers are listed and regularly checked for their compliance with data protection.

13.9.2.4 There is a deletion concept to limit the storage period (deletion rules, responsible persons, deletion periods).

13.9.2.5 The data protection impact assessment (DPIA) is conducted as necessary.

13.9.2.6 The organization adheres to the information obligations according to Art. 13 and 14 GDPR.

13.9.2.7 There is a formalized process for handling information requests from affected individuals and for dealing with data protection incidents.

13.9.2.8 Employees receive confidentiality and data secrecy training annually, or basic data protection training every 2 years. Individual data protection trainings take place in the event of changes in the company context.

13.9.2.9 Central documentation of all procedures and regulations related to data protection with access for employees as needed/authorised (e.g. wiki, intranet ...).

13.9.2.10 No more personal data than necessary for the respective purpose is collected.

13.9.2.11 Declarations regarding the data protection obligations of the processing staff are available.

13.10 Privacy by design and privacy-friendly default settings (Art. 25 para. 2 GDPR)

13.10.1 Limitation of storage period

13.10.2 Restriction of accessibility

13.10.3 Limitation of the scope of processing the data collected

13.10.4 Monitoring of external access (log files)

13.10.5 Use of spam filter and regular updates.

13.10.6 Use of virus scanner and regular updates.

13.10.7 Documented procedure (emergency plans) for dealing with security incidents and formal process and responsibilities for post-processing of security incidents and data breaches.

14. Obligations of the contractor and violation of the protection of personal data

14.1 The contractor shall immediately inform the client about any violations or suspected violations against this contract or regulations concerning the protection of personal data.

14.2 The contractor assists the client in the investigation, limitation, and remedy of the violations.

14.3 Should the personal data, which is processed under this agreement, be endangered by the contractor due to seizure, bankruptcy or comparison proceedings or by other events or measures by third parties, the contractor must immediately inform the client. The contractor will immediately inform all relevant parties that the control over the data lies with the client.

14.4 In the event of inspections by the data protection supervisory authorities, the contractor undertakes to communicate the result to the client, as far as it affects the processing of personal data under this contract. The deficiencies found in the audit report will be immediately rectified by the contractor and the client will be informed about it.

15. Subcontractors

15.1 Subcontracting relationships within the meaning of this regulation are understood to be those services that directly relate to the provision of the main service. This does not include ancillary services which the contractor might use, such as telecommunications services, post / transport services, maintenance and user service, or the disposal of data carriers and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the contractor is obliged to take appropriate and legally compliant contractual arrangements and control measures to ensure data protection and data security of the client's data, even in outsourced ancillary services.

15.2 Outsourcing to subcontractors or changing the existing subcontractor is permissible if the contractor notifies such outsourcing to subcontractors to the client a reasonable time in advance in writing or text form and the client does not object to the planned outsourcing in writing or text form up to the time the data is transferred to the contractor and a contractual agreement in accordance with Art. 28 para. 2-4 GDPR is applied. If the client refuses to consent to the objection for reasons

other than important ones, the contractor may terminate the contract at the time of the planned use of the subcontractor.

15.3 The client agrees to the appointment of subcontractors provided a contractual agreement in accordance with Art. 28 para. 2-4 GDPR. He already agrees to the appointment of the subcontractor named in this chapter.

15.4 The transfer of personal data of the client to the subcontractor and its initial performance is only permitted when all conditions for subcontracting are met.

15.5 If the subcontractor provides the agreed service outside the EU/EEA, the contractor ensures the data protection legality through appropriate measures, No. 2, para. 2. The same applies if service providers in the sense of para. 1 sentence 2 should be used.

15.6 The following subcontractors are part of the approved circle at the conclusion of this contract:

15.6.1 Amazon Web Services, Inc.

Address: 410 Terry Avenue North, Seattle WA 98109, United States;

Purpose: Hosting;

Location of data processing: Germany;

Guarantee: Adequacy decision is available. Amazon.com Inc. is DPF-certified. The use of the tool Amazon Web Services is permissible.

15.6.2 fiskaly GmbH

Address: Mariahilfer Straße 36/5, 1070 Vienna, Austria;

Purpose: Fiscability of invoices;

Location of data processing: EU, Austria;

Guarantee: Order processing contract, tested TOM, listing of tested subcontractors, confidentiality agreement, ISO 27001 certification.

15.6.3 Adyen N.V.

Address: Simon Carmiggeltstraat 6, 1011 DJ, Amsterdam, Netherlands;

Purpose: Payment processing; Location of data processing: Amsterdam, Netherlands;

Guarantee: Order processing contract, tested TOM, listing of tested subcontractors, confidentiality agreement.

16. Deletion and Return of Personal Data

16.1 Upon completion of the processing services agreed upon in the main contract, the Contractor is obliged, at the discretion of the Client, to return or delete all personal data which he received in the course of contract processing. This specifically includes the results of data processing, documents provided and data carriers, as well as copies of personal data. The obligation to delete or return does not apply if the Contractor is legally obligated under EU law or the law of the Member States to continue to store the data. If there is a further obligation to store, the Contractor must restrict the processing of personal data and only use the data for the purposes that require retention. The obligations for the security of processing continue for the duration of the storage. The Contractor must delete the data promptly as soon as the obligation to store expires.

16.2 The deletion must be carried out in such a way that the data cannot be restored.

16.3 The processes must be documented with details regarding the date and the person performing the task. The logs, as well as a written proof of implementation, must be provided to the Client after the processes have been completed.

17. Liability

17.1 The Client ensures within his area of responsibility the implementation of the regulations arising from the relevant applicable legal provisions regarding the processing of personal data.

17.2 In principle, the liability limitations from the main contract apply. The Client indemnifies the Contractor from all claims made by third parties against the Contractor due to the violation of their rights based on the Client's commissioning of personal data, unless the third party's claim is based on the illegal processing of personal data by the Contractor. Article 82 of the GDPR remains unaffected.

18. Miscellaneous, General

18.1 If the personal data of the Client at the Contractor's premises are jeopardized by seizure or confiscation, through insolvency or settlement proceedings, or by other events or measures by third parties, the Contractor shall immediately inform the Client.

18.2 The Contractor will immediately inform all responsible parties in this context that sovereignty over the Client's personal data lies with the Client.

18.3 Irrespective of the Client's right to issue instructions in accordance with paragraph 11 of this Agreement, changes and additions to this Agreement and all its components require a written Agreement and explicit indication that it is an amendment or supplement to these conditions. This also applies to the waiver of this formal requirement.

18.4 The provisions of this Agreement remain in effect even after the termination of the primary service relationship, up to the complete destruction or return of all the Client's personal data to the Client.

18.5 If individual parts of this Agreement are invalid, it does not affect the validity of the rest of this Agreement. The parties agree to replace the invalid provision with a legally permissible provision that most closely fulfills the purpose of the invalid provision.

19. Final Provisions

19.1 Amendments or side agreements require the written form or an electronic format. This also applies to changes to this form requirement.

19.2 If a provision of this Agreement proves to be invalid, this does not affect the validity of the remaining provisions of the Agreement.

19.3 This agreement has been translated into English using artificial intelligence. In case of any discrepancies, ambiguities or disputes, the original German version shall govern and be considered as the definitive and binding document.