Agreement on the processing of personal data on behalf of a controller in accordance with Art. 28 of the General Data Protection Regulation (GDPR)

The Processor:

myhotelshop GmbH

Floßplatz 6

04107 Leipzig

(hereinafter referred to as “MHS”)

Preamble

The Client uses the services offered by MHS to achieve a sustained increase in the direct business of hotels.

In this context, it cannot be ruled out that the Client will process personal data. Under Art. 28 GDPR, it is necessary to conclude a data processing agreement for this purpose which covers the processing of personal data on behalf of a controller.

In order for such processing on behalf of a controller to be permissible under Art. 28 GDPR, the Client must commission MHS to process data. This agreement contains MHS’s commissioning by the Client, and defines the parties’ rights and obligations in connection with this data processing as well as the resulting special obligations with regard to data protection and data security. In principle, the Client shall be responsible for compliance with the provisions of the GDPR and other regulations on data protection and in this respect shall retain control over the data to be processed. Hereinafter the term "Controller" is used for the Client.

1) General

a) MHS shall process personal data on behalf of the Controller within the meaning of Art. 4 No. 8 and Art. 28 of Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR). This agreement defines the parties' rights and obligations in connection with the processing of personal data.

b) Where the term 'data processing' or 'processing' (of data) is used in this agreement, this is based on the definition of 'processing' within the meaning of Art. 4 No. 2 GDPR.

2) Object of the commissioned data processing

This agreement shall apply to all activities that are related to the underlying commissioning and where employees of MHS, or third parties commissioned by MHS, may come into contact with or receive personal data of the Controller. The work and/or services with which the Controller has commissioned MHS is specified in **Annexe 1**. This annexe also indicates the object of the processing, the nature and purpose of the processing, the nature of the personal data, and the categories of data subjects.

3) Obligations of MHS

a) MHS shall process personal data exclusively within the framework of the agreements made and/or in compliance with any supplementary instructions issued by the Controller. This does not apply to legal regulations which may oblige MHS to process the data in a different way. In such a case, MHS shall notify the Controller of such legal requirements prior to the processing, unless the relevant law prohibits such notification due to an important public interest. The purpose, nature and scope of data processing shall otherwise be governed exclusively by this agreement and/or the Controller's instructions. MHS shall be prohibited from processing data in any other way, unless the Controller has agreed to this in writing.

b) As a rule, MHS undertakes to carry out data processing on the Controller's behalf only in Member States of the European Union (EU) or the European Economic Area (EEA).

c) Any transfer of the data processing or use to a third country shall require the Controller's approval and may only take place if the legal regulations – under Sect. 78 ff. of the German Federal Data Protection Act (BDSG) as well as Art. 44 and Art. 49 GDPR – are observed. This concerns, inter alia, any commissioning which requires the use of support platforms. In **Annexe 1**, MHS refers to the applicable privacy notices in this regard. Approval shall be deemed to have been granted if the data processing agreement is approved and the use of the support platforms forms part of the processing.

d) MHS shall inform the Controller without undue delay if, in its opinion, an instruction issued by the Controller violates legal regulations. MHS shall be entitled to suspend execution of the relevant instruction until it has been confirmed or changed by the Controller. If MHS can demonstrate that processing according to the Controller's instruction may lead to liability on the part of MHS pursuant to Art. 82 GDPR, MHS shall be entitled to suspend further processing in this respect until the liability between the parties has been clarified.

4) Reporting obligations of MHS

a) MHS shall be obliged to notify the Controller without undue delay of any breach of data protection regulations or of the contractual agreements and/or of the instructions issued by the Controller which has occurred in the course of the processing of data by it or by other persons employed to carry out the processing. The same shall apply to any breach of personal data MHS processes on behalf of the Controller.

b) Furthermore, MHS shall inform the Controller without undue delay if a supervisory authority takes action against MHS pursuant to Art. 58 GDPR and if this may also involve checking the processing that MHS performs on behalf of the Controller.

c) MHS is aware that the Controller may be bound by a notification obligation under Art. 33 or 34 GDPR, which requires notification to the supervisory authority within 72 hours after knowledge of a violation arises. MHS shall assist the Controller in complying with the notification obligations. In particular, MHS shall notify the Controller of any unauthorised access to the personal data processed on the Controller's behalf, without undue delay as soon as it becomes aware of such access. MHS's notification to the Controller shall include the following information in particular:

a. a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. a description of the measures taken or proposed by MHS to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5) Duties of cooperation on the part of MHS

a) MHS shall support the Controller in its obligation to respond to requests from data subjects to exercise their rights under Art. 12–23 GDPR.

b) MHS shall assist the Controller in its preparation of records of processing activities.

c) Taking into account the nature of the processing and the information available to it, MHS shall assist the Controller in complying with the obligations specified in Art. 32–36 GDPR.

6) Monitoring powers

a) The Controller shall have the right to monitor compliance with the statutory provisions on data protection and/or compliance with the contractual arrangements agreed between MHS and the Controller and/or MHS's compliance with the Controller's instructions, to the required extent.

b) MHS shall be obliged to provide information to the Controller to the extent necessary to carry out the monitoring within the meaning of Paragraph a).

c) MHS and the Controller anticipate that monitoring will be required no more than once a year. The nature and method of the monitoring shall be subject to individual agreement between MHS and the Controller. Further inspections must be justified, stating the reasons.

d) If MHS wishes, proof of compliance with the technical and organisational measures may be provided by submitting an appropriate, up-to-date certificate, reports or report extracts from independent bodies (e.g. data protection officer) or appropriate certification, if the inspection report reasonably enables the Controller to satisfy itself of compliance with the technical and organisational measures in accordance with **Annexe 3** to this agreement.

e) In the case of measures taken by the supervisory authority against the Controller within the meaning of Art. 58 GDPR, in particular with regard to information and monitoring obligations, MHS shall be obliged to provide the necessary information and to enable the competent supervisory authority to carry out an on-site inspection. The Controller must be informed of this.

7. Subcontractual relationships

a) MHS shall be entitled to use the subcontractors specified in **Annexe 2** to this agreement to process data on its behalf. Any change of subcontractors or the appointment of further subcontractors shall be permitted under the conditions set out in Paragraph b).

b) MHS shall select the subcontractor carefully and check before commissioning that the subcontractor is able to fulfil the agreements made between the Controller and MHS. MHS must in particular check in advance, and regularly during the contract period, that the subcontractor has taken the technical and organisational measures necessary for the protection of personal data in accordance with Art. 32 GDPR. If there

are plans to change a subcontractor or commission a new one, MHS shall inform the Controller in text form in good time, but no later than four weeks prior to the change or the new commissioning (“Information”). The Controller shall be entitled to object to the change or the new commissioning of the subcontractor in text form within three weeks after receipt of the Information, stating the reasons. The Controller shall be entitled to withdraw its objection at any time in text form. In the event of an objection, MHS shall be entitled to terminate the contractual relationship with the Controller by giving least 14 days’ notice to the end of a calendar month. MHS shall take reasonable account of the Controller’s interests when determining the notice period. If the Controller does not object within three weeks of receipt of the Information, the Controller shall be deemed to have consented to the change or new commissioning of the subcontractor concerned. The Controller shall be informed separately in the Information of the consequences of not responding.

c) MHS shall be obliged to have the subcontractor confirm that it has designated a company data protection officer in accordance with Art. 37 GDPR, insofar as the subcontractor is legally obliged to designate a data protection officer. If the subcontractor is unable to designate a data protection officer, it shall be obliged to use MHS’s data protection officer, or the data protection agency used by MHS.

d) MHS shall ensure that the arrangements agreed in this contract and, if applicable, any supplementary instructions issued by the Controller, also apply to the subcontractor.

e) MHS shall conclude a data processing agreement with the subcontractor that meets the requirements of Art. 28 GDPR. In addition, MHS shall impose the same personal data protection obligations on the subcontractor as are specified between the Controller and MHS. A copy of the data processing agreement shall be made available to the Controller upon request. Electronic transmission shall be sufficient in this respect.

f) MHS shall in particular be obliged to ensure by contractual regulations that the monitoring powers of the Controller and of supervisory authorities also apply to the subcontractor and that corresponding monitoring rights of the Controller and of the supervisory authorities are agreed. It must also be contractually stipulated that the subcontractor shall be required to tolerate these monitoring measures and any on-site inspections.

g) Subcontractual relationships within the meaning of Paragraphs a) to f) shall not include third-party services which MHS uses as purely ancillary services in order to carry out its business activities. This includes, for example, cleaning services, pure telecommunication services without concrete reference to services that MHS provides for the Controller, postal and courier services, transport services, guarding services. MHS shall nevertheless be obliged to ensure that appropriate precautions and technical and organisational measures have been taken to guarantee personal data protection, even in the case of ancillary services provided by third parties.

8. Obligation to maintain confidentiality

a) When processing data for the Controller, MHS shall be obliged to maintain confidentiality in respect of data which it receives or becomes aware of in connection with the order.

b) MHS has familiarised its employees with the relevant data protection provisions and required them to provide an undertaking to maintain confidentiality.

c) Upon request, MHS shall be required to prove to the Controller that its employees have provided the undertaking according to Paragraph b).

9) Safeguarding the rights of data subjects

a) The Controller shall be solely responsible for safeguarding the rights of data subjects. MHS shall be obliged to support the Controller in its duty to process requests from data subjects under Art. 12–23 GDPR. In this context, MHS shall in particular

ensure that the information required in this respect is made available to the Controller without undue delay so that the latter can in particular comply with its obligations under Art. 12(3) GDPR.

b) Insofar as MHS's cooperation is necessary for the Controller to be able to safeguard the rights of data subjects, in particular the right of access and the rights to have data rectified, blocked or erased, MHS shall take the necessary measures according to the Controller's instructions. MHS shall take appropriate technical and organisational measures to support the Controller as far as possible in fulfilling its obligation to respond to requests from data subjects to exercise their rights.

c) This shall not affect provisions on any remuneration of additional expenses incurred by MHS for its cooperation when data subjects exercise their rights vis-à-vis the Controller.

10) Remuneration

The remuneration owed to MHS shall be agreed separately.

11) Technical and organisational measures for data security

a) MHS hereby assures the Controller that it shall comply with the technical and organisational measures that are necessary to comply with the applicable data protection regulations. This includes in particular the requirements of Art. 32 GDPR.

b) The status of the technical and organisational measures in place at the time of contract conclusion is attached as **Annexe 3** to this agreement. MHS and the Controller agree that changes to the technical and organisational measures may be necessary in order to adapt to technical and legal circumstances. MHS shall agree in advance with the Controller any significant changes that may affect the integrity, confidentiality or availability of personal data. MHS may implement measures without consulting the Controller if this involves only minor technical or organisational changes and does not adversely affect the integrity, confidentiality and availability of personal

data. The Controller may request an up-to-date overview of the technical and organisational measures taken by MHS once a year, or when it has justified reasons for doing so.

12) Duration of the processing on the Controller's behalf

a) The agreement shall begin upon approval and run for the duration of the main contract concluded between the parties on the Controller's use of MHS's services.

b) The Controller may terminate the agreement at any time without notice if there is a serious breach by MHS of the applicable data protection regulations or of obligations arising from this agreement, if MHS is unable or unwilling to carry out an instruction from the Controller, or if, in breach of the agreement, MHS refuses entry to the Controller or the competent supervisory authority.

13) Termination

After termination of the agreement, MHS shall be required, at the Controller's discretion, to either return or erase all documents, data and processing or usage results that are related to the processing performed on the Controller's behalf and have come into its possession. The erasure shall be documented in an appropriate manner. This shall not affect any statutory retention obligations or other obligations to store the data.

14) Final provisions

a) This agreement is subject to German law.

b) Ancillary agreements shall require the written form.

c) Should individual parts of this agreement be invalid, this shall not affect the validity of the remaining provisions of the agreement.

Leipzig, 15 April 2021

Ullrich Kastner

Managing Director of myhotelshop GmbH

Annexe 1

Services provided by MHS: Scope, nature and purpose:

Creation of placements (campaign selection, setup and optimization), consulting and management (online direct sales strategy development) and website services (stronger conversions and enhanced booking experiences).

Types of data:

Any data stored by MHS in connection with the contractual relationship, in particular that of its business clients, their employees, namely names, addresses, email addresses, telephone numbers if applicable, as well as details of contact use and order fulfilment.

Data subjects:

Employees of the contractual partners, as well as customers of the hotels.

Use of support platforms, by MHS or third parties identifiable from the subcontractual relationship, for the provision of the contracted services:

For their part, the support platforms constitute separate companies which, as of 25 May, work and operate in a GDPR-compliant manner. MHS has to assure this fact from the moment of the cooperation between MHS and the support platform / company. These companies can be contacted separately by the Controller. The Controller is also entitled to request information via MHS about the Controller's personal data, after stating a justified and substantiated reason.

- easybill, easybill GmbH, Düsselstr. 21, 41564 Kaarst, Germany, https://www.easybill.de/en/privacy

- Google Ads, Google Tag Manager, Google Analytics and associated applications, Google Germany GmbH, ABC-Straße 19, 20354 Hamburg, Germany, https://policies.google.com/privacy
- Microsoft Advertising, Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 Munich, Germany, https://privacy.microsoft.com/en-US/privacystatement
- Matomo, ePrivacy Holding GmbH, Große Bleichen 21, 20354 Hamburg, Germany, https://matomo.org/privacy-policy/
- Mailchimp, The Rocket Science Group LLC d/b/a Mailchimp, 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308, US, https://mailchimp.com/legal/privacy/
- Pipedrive, Pipedrive OÜ, Mustamäe tee 3a, Tallinn 10615, Estonia, https://www.pipedrive.com/en/privacy

The support platforms mentioned above may apply tracking technologies which measure the provision of the service and thus lead to the billability of the same. Tracking devices:

- Cookies which create the following records: location / user agent (information about the browser itself) / time and duration of access

Use of tools:

- Coupon tools
- Chat tools
- Newsletter subscription forms
- Contact forms
- Web font libraries

Annexe 2

MHS currently uses the following subcontractors:

- Mittwald CM Service GmbH & Co. KG, Königsberger Straße 4-6, 32339 Espelkamp, Germany, https://www.mittwald.de/datenschutz

Annexe 3

Technical and organisational measures at MHS

MHS takes the following technical and organisational measures for data security within the meaning of Art. 32 GDPR:

1) Confidentiality

a) Physical access control

Unauthorised persons are physically denied access to data processing systems used to process or use personal data:

Storage of data in a data centre / on a server that is not generally accessible, and there:

- Electronic physical access control system with logging
- Documented allocation of keys to employees
- Guidelines for accompanying guests in the company
- Staffing of data centres during business hours and permanent availability of the persons responsible for them.

b) Equipment access control

Unauthorised use of data processing systems must be prevented:

- Implementation by means of user account control, access to IT systems only possible with username and password
- MHS assigns passwords itself, which can be changed again after initial use.

c) Data access control

It must be ensured that persons authorised to use a data processing system can only access personal data subject to their access authorisation, and that data cannot be read, copied, changed or removed without authorisation during processing, use and storage.

- Establishment of an authorisation concept in which individual clients are exclusively assigned access to their own areas and data
- Logging of access in log files of MHS or third parties
- The Controller is responsible for maintaining the confidentiality of the access data and, if applicable, for passing it on to employees.

d) Physical, equipment and data access control for and from a third country

Should MHS deem it necessary, the following measures to secure physical access, equipment access and data access will be considered and applied:

- Encryption
- Pseudonymisation
- Read-only access from the third country.

e) Separation control

It must be ensured that data collected for different purposes can be processed separately:

- Controller data is stored in a physically or logically separate manner from other data
- Data backup is also done physically or logically.

2) Integrity

a) Input control

It must be ensured that it can be examined and established later on whether and by whom personal data has been entered, changed or deleted in data processing systems:

- The data is entered and processed by MHS itself
- Access for MHS is logged; this applies in particular to access to databases or systems of the Controller in which personal data is stored.

b) Data transmission control

It must be ensured that personal data cannot be read, copied, changed or deleted by unauthorised persons when transferred electronically or while being transported or stored on data carriers, and that it can be examined and established where personal data is to be transmitted by data transmission equipment.

- Employees are obliged to maintain confidentiality under the GDPR and/or Sect. 53 BDSG (new)
- The transmission of data from and to the Client areas only occurs using SSL encryption
- The Controller is responsible for setting up transmission paths to external systems (data export).

3) Availability and resilience

It must be ensured that personal data is protected against accidental destruction or loss.

- Controller data is subject to regular data backups
- Use of redundant systems
- Use of uninterruptible power supply.

4) Procedures for regular review, assessment and evaluation

MHS employees are instructed in data protection law at regular intervals and they are familiar with the procedural instructions and user guidelines for data processing on behalf of the Controller, including with regard to the principal's right to issue instructions. Each employee is required to provide a written undertaking to comply with data protection requirements under the GDPR no later than on the first day at the start of his or her employment. The employee does not have access to personal data before providing such an undertaking.