MCI

Data protection standard contractual clauses for subcontracting - Hotel

PERSONAL DATA / PROCESSOR

I. The purpose of these clauses is to define the conditions under which **the Hotel (data processor)** undertakes to carry out the personal data processing operations defined below on behalf of **MCI, the data controller**.

As part of their contractual relationship, the parties undertake to comply with the regulations in effect applicable to personal data processing and in particular, Regulation (EU) 2016/679 applicable from 25 May 2018 (hereinafter the "General Data Protection Regulation" or "GDPR").

Under the terms of this rider, the following terms are defined as follows:

- "data controller": the natural person or legal entity, public authority, service or other organisation which, solely or jointly with others, determines the purposes and methods of processing; where said processes and methods are determined by European Union law or the law of a Member State, the controller may be appointed or the specific criteria applicable to their appointment may be provided for by European Union law or the law of a Member State.
- "processor": the natural person or legal entity, department or other organisation that processes personal data on behalf of the data controller.

II. Description of the processing carried out by processors

The processor is authorised to process personal data on behalf of the data controller that are necessary to provide the following service(s) – Hotel booking.

The details of the processing carried out by processors are as follows:

Purpose(s) of processing	Hotel booking
Categories of personal data processed	Rooming list: Name, Surname, email address, country of origin, company name, arrival and departure dates
Categories of persons concerned	Congress participants

Period of data retention or criterion justifying the retention of data (separate from the term of the contract)	Maximum 1 year after departure date
Processor contact person	Signatory of the contract

This rider is valid as a written instruction for the processing of data by the processor.

III. Processor's obligations in respect of the data controller

The processor undertakes to:

1. process the data solely for the purpose(s) of the subcontracting

2. process the data in accordance with the data controller's documented instructions. If the processor considers that an instruction constitutes an infringement of the General Data Protection Regulation or any other provision of European Union law or the law of Member States on data protection, it must inform the data controller immediately.

3. unless otherwise specifically and expressly authorised by the data controller, process data exclusively within the territory of an EEA Member State. The processor undertakes not to disclose, make accessible or transfer any of the data controller's data, even for routing purposes, to any processing organisation or processor based in a country located outside the EEA, except with the data controller's prior written consent.

The data controller reserves the right to carry out any checks it deems necessary to confirm the performance of the obligations arising under this clause.

In the event of a transfer outside the EEA, authorised by the data controller, said transfer may only take place within the strict limits necessary for the performance of the services, and provided said transfer is towards a State whose legislation in respect of personal data protection has been recognised by the European Commission as offering an equivalent level of protection, or is governed by standard contractual clauses issued by the European Commission or is carried out on the basis of any other alternative arrangements recognised by the General Data Protection Regulation, subject to data controller's prior agreement to said arrangements in writing. The subcontractor undertakes to append to the present contract the documentary evidence allowing him to make such a transfer.

The processor will ensure that its own processors sign and comply with the requirements of this clause.

4. guarantee the confidentiality of the personal data processed under this contract

5. ensure that those authorised to treat personal data according to this contract:

 undertake to respect confidentiality or are subject to an appropriate statutory confidentiality obligation

 receive the necessary training in respect of personal data protection

6. take account of data protection principles and data protection by default from the design stage onwards of tools, products, applications and services

IV. Subcontracting

The processor may call on another processor (hereinafter "the subsequent processor") to carry out specific processing activities. In this case, they must inform the data controller in advance, and in writing, of any planned changes with regard to adding or replacing other processors. This information must clearly indicate the processing activities subcontracted, identity and contact details of the processor and dates of the subcontracting agreement. The data controller has a minimum period of one (1) month from the date of receipt of said information to present its objections. Said subcontracting may only proceed if the data controller has not expressed an objection during the agreed period.

The subsequent processor is obliged to fulfil the obligations set out in this contract on behalf of the data controller and in accordance with their instructions. It is the initial processor's responsibility to ensure that the subsequent processor offers the same sufficient guarantees in respect of the implementation of appropriate technical and organisational measures to ensure that the processing meets the requirements of the General Data Protection Regulation. Should the subsequent processor fail to fulfil their obligations in respect of data protection, the initial processor shall retain full responsibility in respect of the data controller for the other processor's fulfilment of its obligations.

V. Data subjects' right to information

In the event that the data controller authorises the processor to this effect, it will be the latter's responsibility to provide information relating to the data processing carried out by it to the data subjects concerned by the processing operations at the time the data are collected. The formulation and format of the information must be agreed with the data controller before the data are collected.

VI. Exercise of individual rights

So far as possible, the processor must help the data controller to fulfil its obligation to respond to requests to exercise their rights by data subjects, including rights of access, correction,

deletion and opposition, right to restriction of processing, right to data portability and right not to be the subject to an automated individual decision (including profiling).

Should the persons concerned make a request to exercise their rights to the processor, said processor must send such requests, on receipt, by e-mail to anne.lesca@mci-group.com, MCI Data Protection Officer.

VII. Notification of breaches of personal data

The processor must notify the data controller of any personal data breach within a maximum of 24 hours after becoming aware of it, by e-mail to the data protection officer. Said notification must be accompanied by any documentation that may be useful in enabling the data controller to inform the relevant regulatory authority of the breach, if applicable.

The processor must, throughout the period of the Contract, set up and maintain a process and procedures to manage security incidents (including, in particular, breaches of personal data) and ensure continuity of service in accordance with industry standards. The processor (i) shall notify the data controller of the name and contact details of one of its employees, who shall act as the data controller's primary point of contact in respect of security issues and be available 24/7 to deal with any security incidents. Any request from the data controller relating to security must be treated diligently and as a priority by the processor.

Without prejudice to the data controller's other rights and remedies, in the event of a presumed or proven security incident or breach of personal data, the processor must advise the data controller immediately and at the latest, within 24 hours following the occurrence of the security incident or breach of personal data.

Immediately after said notification, the Parties will coordinate their actions in order to investigate the security incident concerned. The processor undertakes to cooperate fully with the data controller, at its own expense, to help it to manage the situation, including but not limited to: (i) helping it with any investigation; (ii) providing the data controller or an independent third party appointed by the data controller with physical access to the facilities and operations concerned; (iii) organising interviews with the employees of the data controller and all other appropriate individuals; and (iv) providing all registers, logs, files, data communications and other relevant documents necessary for compliance with laws, regulations and industry standards or as required by the data controller.

The processor will also provide all reasonable assistance to the data controller in the case of a notification in respect of any action the latter may be obliged or may choose to take in respect of a personal data breach. The processor undertakes not to inform third parties, including the persons concerned, of any breach of personal data without having obtained the prior consent of the data controller in writing, except in the cases provided for in the General Data Protection Regulation. Moreover, the processor acknowledges that the data controller has sole authority to determine: (i) whether or not the breach of personal data must be notified to any individual, regulatory authority, administrative authority or other person pursuant to the General Data Protection Regulation; and (ii) the content of said notification. Where the General Data Protection Regulation requires that the data controller notify the breach of personal data to the

persons concerned, it is understood that the processor will bear all the costs associated with said notification.

The processor shall take the appropriate measures, at its own expense, to mitigate the consequences of any security incident and remedy it, and shall make all the amendments it judges necessary in order to avoid any reoccurrence of an incident of this kind. The processor shall assist the data controller, at its own expense, with restoring the data controller's data in the event of a data loss caused by any failure to fulfil its regulations in respect of the Contract.

The processor shall cooperate and provide the data controller with the necessary assistance in respect of any complaint formulated by a data subject or any investigation or request issued by a regulatory authority with regard to the General Data Protection Regulation or any other applicable regulation.

The processor will reimburse the data controller for the actual costs the latter incurs in providing a response to any security incident and mitigating the harm caused as a result of said incident including, among other things, the cost of investigations, notifications and/or corrective measures. Where the General Data Protection Regulation requires the data controller to notify a breach of personal data, the processor will cover the costs associated with said notification.

It is expressly agreed between the Parties that in the event of a breach of personal data, the following harm shall be deemed direct: (i) reasonable and necessary expenses for investigation and remediation; (ii) reasonable and necessary costs of notification, where such a notification is required by the applicable regulations and (iii) penalties, damages, amounts paid in respect of settlements, reimbursements, compensation and other costs related to the fulfilment of obligations arising from a judgment, settlement or the applicable regulations (the "Losses"), insofar as said losses are due to a failure by the processor to fulfil its contractual obligations.

The processor shall maintain a record of security incidents and make this available to the data controller, including but not limited to breaches of personal data, and shall document all relevant information concerning the circumstances of said incidents and breaches, the harm caused and corrective measures taken to mitigate their effects, as well as the actions and measures taken to avoid any repetition of such incidents or breaches.

VIII. Assistance from the processor in relation to the data controller's fulfilment of its obligations

The processor shall cooperate with the data controller and use its best endeavours to help the data controller prove that it is compliant with all its legislative and regulatory obligations, notably in respect of the General Data Protection Regulation.

In particular, the processor shall, where relevant, assist the data controller with carrying out impact analyses in respect of data protection.

The processor shall, where relevant, also assist the data controller in carrying out a prior consultation with the regulatory authority.

IX. Security measures

The processor acknowledges that security is a fundamental criterion for the data controller and that the processor's compliance with the security requirements defined in the schedule to this contract is an essential and decisive obligation for the data controller's consent thereto.

The Processor undertakes to detail in annex to this contract the security measures taken to ensure the security of the processing of personal data carried out on behalf of the data controller, in accordance with article 32 of the GDPR.

X. Retention of data

Once the provision of services relating to the processing of these data is complete, the processor undertakes to:

- Destroy all personal data or
- At any time, at the data controller's written request and at the latest, within 15 calendar days of the end of the Contract, the processor undertakes to return the data controller's personal data, in a legible or interoperable form agreed between the Parties and to destroy all copies (paper or electronic) of the data controller's personal data that it may hold.

The return of all files, data, programmes, documentation, etc. is included in the price for the provision of the Service.

The processor must confirm the actual destruction of the data controller's personal data within 15 calendar days of the data controller's request or the end of the Contract.

The data controller reserves the right to carry out any checks it deems necessary to confirm the performance of these obligations.

This clause will remain in effect after the expiry or termination of the Contract for any reason whatsoever.

XI. Register of categories of processing activities

The processor declares that it holds a written record of all categories of processing activities carried out on behalf of the data controller including:

• the name and contact details of the data controller on behalf of whom it is acting, any processors and, if applicable, the data protection officer;

- the categories of processing activities carried out on behalf of the data controller:

- if applicable, any transfers of personal data to a third country or international organisation, including the identification of said third country or international organisation and, in the case of transfers referred to in clause 49, paragraph 1, second subparagraph of the General Data Protection Regulation, documents attesting to the existence of appropriate guarantees;

- as far as possible, a general description of technical and organisational security measures, including but not limited, as required, to:

  - pseudonymisation and encryption of personal data;
  - means of guaranteeing the constant confidentiality, integrity, availability and resilience of processing systems and services;
  - means of re-establishing the availability of personal data and access thereto in an appropriate time frame in the event of a physical or technical incident;
  - a procedure for regularly testing, analysing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

XII. Documentation

The processor shall provide the data controller with the necessary documentation to demonstrate compliance with all its obligations and to enable audits and inspections to be carried out by the data controller or another auditor appointed by it, and to contribute to said audits.

XIII. Audit

Throughout the term of the Contract, the data controller may carry out tests and audits of all or some of the services, either itself or through an independent third party at its expense – subject to five (5) working days' notice – including at the premises of authorised processors, in order to ensure compliance with the stipulations of the Contract in terms of:

- compliance with Security Policies,
- quality of service,
- maintenance of appropriate security measures, in particular to ensure the integrity and confidentiality of the Data Controller's data.

Where the services involve the processing of personal data, the audit may also relate to the verification of the General Data Protection Regulation and the verification of:

- locations used for the processing and/or storage of personal data;
- transfers of personal data outside the European Economic Area;
- measures taken to ensure the security of personal data and combat breaches of personal data.

The processor undertakes to authorise the data controller, or the companies appointed by the latter and tasked with carrying out the audit, to access the necessary information to carry out their mission properly and access the sites where the services are delivered.

The processor will cooperate fully (and, where processors and representatives are concerned, ensure their cooperation) with the data controller and, depending on the case, the audit representatives of the data controller, including giving them access to the premises, personnel, physical and technical environments, equipment, software, documentation, data, registers and systems relating to the services, and any useful information that might reasonably be necessary in carrying out the audit.

An audit report must be sent to the processor.

The processor also authorises the data controller to carry out or arrange for security tests to be carried out continuously to check that the processor's systems are not vulnerable (for example, because of a defective configuration or update) and detect any change likely to expose data to the risks of intrusion.

Moreover, the data controller may carry out any investigations on the internet to detect proven breaches of personal data.

Should it become apparent, following the audit and testing measures described above, that the security measures implemented by the processor are not appropriate or sufficient, or if said audits or tests reveal any gaps or examples of non-compliance with the requirements set out in this Contract and/or the legal requirements applicable and/or the standards in effect, the processor will implement corrective actions within a time frame to be agreed between the Parties, depending on the severity of the failure observed and in any case, not longer than 15 days, without prejudice to the data controller's additional rights to seek damages and/or terminate the Contract. Audit costs will be payable by the processor in the event of any failings identified in the audit.

XIV. Data controller’s obligations in respect of the processor

The data controller undertakes, throughout the term of the contract, to:

1. provide the processor with the data referred to in clause II;

2. document in writing any additional instructions regarding the processing of data by the processor;

3. ensure, prior to and during the period of processing, compliance with the obligations set out in the General Data Protection Regulation by the processor;

4. supervise the processing, including carrying out audits and inspections at the processor’s premises in accordance with the provisions of this rider.