

AGREEMENT ON THE PROCESSING OF PERSONAL DATA

This agreement on the processing of personal data (“Annex”) constitutes a part of the General contractual terms (“Agreement”) between Domainhotelli Oy (“Service provider”) and the customer (“Customer”).

1. Initial information

The purpose of this Annex is to agree on the obligations under the relevant personal data regulations between the Service provider and the Customer. This Annex constitutes a written agreement between the parties on the processing of personal data in accordance with the EU General Data Protection Regulation (679/2016). The obligations and rights related to the EU Data Protection Regulation will not enter into force until the application of the EU General Data Protection Regulation starts on May 25, 2018.

According to the Agreement, the Service provider provides the services (“Service”), including, but not limited to, hosting services and/or support services to the Customer. The service can be used for storing and/or processing Personal data. This also applies to the Personal data of the Customer. The Customer acts as the Data controller with regards to the Personal data processed in these Services. The Service provider acts as the processor for such Personal data.

2. Definition

The terms used within this Annex shall be applied according to the definitions specified in the Agreement. In addition, the following terms have a specific meaning in this Annex:

“Data controller” refers to the Customer who determines the purpose and means of processing personal data.

“Regulation” refers to any national data protection law, the General Data Protection Regulation of the EU (2016/679, “GDPR”) from its date of application (May 25, 2018), and any future applicable data protection legislation.

“Model contractual clauses” refers to the standard contractual terms approved by the European Commission for the disclosure of personal data from EU Data controllers to third country processors (decision 2002/16 EC).

“Personal data” refers to any information relating to an identified or identifiable natural person; an identifiable natural person is a person who can be identified, directly or indirectly, in particular by means of identification data such as name, personal identification number, location data, online identification or one or more characteristic physical, physiological, genetic, psychological, economic, cultural or social factor.

“Processor” refers to the Service provider that processes personal data on behalf of the Customer.

“Processing” refers to any activities in which Personal data is processed.

“Subcontractor” refers to a processor that performs Processing in accordance with this Annex on behalf of the Service provider or Customer.

3. Responsibilities of the Service provider

The Service provider Processes the Personal data of the Customer on behalf of the Customer on the basis of the Agreement. The Service provider shall undertake to comply with the applicable legislation, regulations and authorities’ provisions and guidelines for the Processing of Personal data valid in Finland and the European Union and, if necessary, amend the provisions of this Annex to comply with them.

The Service provider does not specify the type of personal data stored by the Customer on the Service. The Service provider shall not be responsible for how such information is classified, how they are available or exchanged with other parties or otherwise Processed. The Service provider Processes the Personal data solely on behalf of the Customer, and only to the extent and manner specified in the Agreement and Annex or as separately instructed by the Customer. The separate guidelines of the Customer shall be documented in connection with the order, Service description, support request or other written communication.

If the Service provider has reasonable grounds to suspect that the guidelines provided by the Customer conflict (i) with the applicable laws or regulations, and/or (ii) with the provisions of the Agreement or this Annex, the Service provider shall inform the Customer of this without undue delay. The Service provider shall be entitled to postpone the implementation of the guidelines until the Customer amends its guidelines or a separate agreement has been reached regarding the implementation between the Service provider and the Customer.

3.1 Requests from Data subjects or authorities

The Service provider shall immediately inform the Customer about all requests from Data subjects or authorities regarding the revision, correction, deletion or Processing prohibition of the Personal data, or about other requests from Data subjects related to exercising the rights of the Data subject stipulated in current legislation and the EU General Data Protection regulation. The Customer shall be obliged to respond to these requests. Taking the nature of the Processing activity into account, the Service provider shall help the Customer with appropriate technical and organisational measures, where possible, for fulfilling the Customer's obligation to respond to the requests of Data subjects.

Taking the nature of the Processing of the Personal data and the data being accessible into account, the Service provider shall be obliged to assist the Customer in ensuring compliance with its statutory obligations. These obligations may include obligations relating to data security, notification of data security breaches, data security impact assessments and prior consultation. The Service provider shall be obliged to assist the Customer to the extent stipulated by the applicable data protection law. Unless otherwise agreed, the Service provider shall be entitled to invoice the costs arising from the activities related to this section of the Annex in accordance with its current price list. In addition, the Service provider shall be given a reasonable time to assist the Customer.

The Service provider shall forward all inquiries from data protection authorities directly to the Customer, and the Service provider shall not have authority to represent the Customer or act on behalf of the Customer with the supervisory data protection authorities.

3.2 Service provider and Regulatory compliance

The Service provider shall comply with the provisions applicable to its own activities and the provision of Services, privacy and security laws, as well as the obligations under this Annex. However, the Service provider shall not be responsible for complying with the laws applicable to the Customer or the industry of the Customer if that legislation is not generally applicable to information technology providers. If required by law, the Service provider shall appoint a data protection officer who shall fulfil his or her duties in accordance with the applicable law.

The information regarding the data protection officer shall be provided to the Customer upon request. The Service provider shall maintain all necessary reports and, at the request of the Customer, make available all information necessary to demonstrate compliance with this Annex and the Legislation.

4. Responsibilities of the Customer

The Customer shall undertake to comply with the applicable legislation, regulations and authorities' provisions and guidelines for the Processing of Personal data valid in Finland and the European Union and, if necessary, amend the provisions of this Annex to comply with them.

The Customer shall be responsible for ensuring the necessary rights and consents to the Processing of Personal data under the Agreement. The Customer shall be responsible for the preparation and availability of a privacy policy, and for informing the Data subjects and notifying data protection authorities.

The Customer shall define the type of Personal data stored on the Services. The Customer shall also determine how the Personal data is used, exchanged or otherwise Processed. The Customer shall be responsible for the integrity, security, maintenance and proper protection of the Personal data, as well as for ensuring that the Customer follows all applicable data protection, data security and security laws and provisions.

5. Technical and organisational measures

The Service provider shall take appropriate technical and organisational measures to protect the Personal data of the Customer, taking into account the risks of the Processing, in particular regarding the accidental or unlawful deletion, loss, modification, disclosure or access to transferred, stored or otherwise Processed Personal data. The implementation of security measures shall take into account the available technical options and their costs in relation to the specific risks associated with the Processing, as well as the sensitivity of the Processed Personal data.

The Customer shall be obliged to ensure that the Service provider is informed of all aspects related to the Personal data provided by the Data controller, such as risk assessments and the processing of special categories of persons who affect the technical and organisational measures under this Annex. The Service provider shall ensure that the personnel of the Service provider or the subcontractor of the Service provider are bound by an appropriate confidentiality obligation.

The implemented data security measures are defined in the minimum data security requirements of the Service provider described in more detail on the website of the Service provider (www.domainhotelli.fi). The Customer shall be obliged to inform the Service provider of any matters (including specific risks or categories of personal data) that require the definition and agreement of additional technical or organisational security measures in the Agreement.

The Customer shall be responsible for the implementation and maintenance of security measures and other technical and organisational safeguards. The measures shall be proportionate to the nature and quantity of Personal data stored and/or otherwise Processed by the Customer. The Customer shall also be responsible for the personnel for whom the Customer has provided access to or usage rights to the Services. The Customer shall also be responsible for third parties having access to the Personal data or the Service, even if the Customer has not taken the necessary security measures, and they have not given permission to process the data.

6. Reporting a security breach

The Service provider shall inform the Customer of any breach of the Personal data without undue delay after obtaining such information, or when the subcontractor of the Service provider has been informed of the breach. The Customer shall be responsible for the necessary notifications to the data protection authorities. The Customer shall also be responsible for notifying the Service provider accordingly of encountered security breaches.

At the Customer's request, the Service provider shall, without undue delay, provide the Customer with all relevant information related to the breach. In so far as that information is available to the Service provider, the Service provider shall provide at least:

- a description of the security breach,
- a description of the likely consequences of the breach, and
- a description of the corrective measures that the Service provider has performed or will perform to prevent such breaches in the future if the security breach has been caused by the Service provider and, where appropriate, the measures for minimising the adverse effects of a potential security breach.

The Service provider shall document and forward the results of the report, as well as the measures taken, to the Customer.

7. Audit

The Customer or an appointed auditor (not a competitor of the Service provider) shall be entitled to audit the activities under this Annex. The parties agree on the time and other details of the audit well in advance and no later than 14 working days before the audit. The audit shall be carried out in a manner that does not adversely affect the commitments of the Service provider and its subcontractors to third parties. The usual confidentiality agreements shall be signed by the representatives of the Customer and the auditor.

The Customer shall be responsible for all costs of auditing. The Service provider shall have the right to invoice the cost of the work performed in the audit to the Customer.

7. Subcontractors

The Service provider shall have the right to use subcontractors for Processing the Personal data of the Customer. The Service provider shall be responsible for the activities of the subcontractors, and prepare corresponding written agreements with the subcontractors on the Processing of Personal data. Upon request, the Service provider shall notify the Customer in advance of the subcontractors it intends to use for the Processing of Personal data under the Agreement. The Customer shall have the right to object to the use of the new subcontractor for legitimate reasons. If the Customer does not oppose the addition or replacement of the subcontractor in writing, it shall be interpreted as accepting the replacement of that subcontractor. If the parties do not reach an agreement on the use of a new subcontractor, the Customer shall have the right to terminate the Agreement with a thirty (30) days' notice to the extent that the subcontractor replacement affects the Processing of the Personal data.

8. Server centre location and data transfer

The server centres of the Service provider, where all personal data are stored and Processed, are mainly located in Finland. However, the Service provider may transfer the Personal data to any data centre located in the EU/EEA, as well as data centres located outside the EU/EEA, as described in the Service description or agreed in connection with the Agreement. The transfer of Personal data outside the EU/EEA shall be governed by the Standard contractual clauses attached to this Annex, or any other transfer mechanism permitted by the Legislation. The Standard contractual clauses shall constitute a part of this Annex and supersede all the provisions of the Agreement or this Annex that are in contradiction.

9. Other terms and conditions

If material or non-material damage is caused to a person due to an infringement of the EU data protection regulation, the Service provider shall be liable for the damage only to the extent that it has not expressly complied with the EU data protection regulation or the obligations of this Annex.

Either party shall be liable to pay the damages and administrative fines imposed only for the part corresponding to the liability for the damage established in the final decision of the data protection supervisory authority or the Court of Justice. In other respects, the parties' liability shall be defined under the Agreement.

The Service provider shall inform the Customer in writing of any changes that may affect its ability or potential to comply with this Annex and the written instructions provided by the Customer. The parties shall agree on all additions and amendments to this Annex in writing.

The Annex shall be valid (i) for as long as the Agreement is in force or (ii) the parties have obligations to each other under the Personal data Processing activities.

Obligations which, by their nature, are intended to remain in force irrespective of the expiry of this Annex shall remain in force after the expiry of the Annex.