HOTEL PERRAKIS

DATA PROTECTION POLICY

of Hotel Perrakis SA

with registered seat in Kypri, Andros, Cyclades, Greece

hereinafter “the Company”

1.1 **INTRODUCTION-DEFINITIONS**

1.2 Purpose of the present Data protection Policy is the compliance with the European General Data Protection Regulation (EU) 2016/679 (**"GDPR**"), in every case of processing of personal data of natural persons.

“**Personal Data”** means information that relates to an identified or identifiable living individual held either on computer or in other electronic or automatically processable form, or in a paper filing system.

“Processing” means collecting, storing, analysing, using, disclosing, archiving, deleting or doing absolutely anything else with Personal Data.

1.3 Company Processes Personal Data regarding its clients, suppliers as well as its employees and individual contract workers, and other individuals (referred to in this policy as **Data Subjects)** in the course of its business.

2. COMPLIANCE WITH THIS POLICY

The Company Processes Personal Data as per the present Data protection Policy and according with the following:

- the purposes of the processing and their other rights are is notified to its employees and other Data subjects.

- The data are processed in a lawful and legitimate way, with transparency and proportionality regarding the scope of the processing.

-Data should be precise, up-to-date, secure and not be kept for a time period longer than what is required.

For the processing of sensitive data and the transfer of data outside the EU the terms of the present policy shall apply.

2.1 The Company will only process Personal Data in a legitimate way and for specific and clear purposes according to its lawful interest, in the framework of implementation of its contractual relationship with the Data Subject, or the Processing doesn't affect or has a minor affect on the Data Subjects it concerns.

The Processing may also be based on the consent of subject, or be in conformity with the Law or take place in fulfillment of a legal obligation.

2.2 The Company will not process Personal Data which are irrelevant or inadequate or exceed what is necessary with Treatment only that with the Consent of Data Subject. The Company actualizes the Personal Data that are not in effect more.

3. SENSITIVE PERSONAL DATA

3.1 The Company processes sensitive data only in accordance with the terms defined each time by the Law. "Sensitive Personal Data"- are Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data and biometric data Processed for the purpose of uniquely identifying a living individual, Personal Data concerning a living individual's health, sex life or sexual orientation, and Personal Data relating to criminal convictions and offences or related security measures.

3.2 When extensive harm may be caused to the Data Subject from the processing of Sensitive Personal Data special measures, such as anonymization will need to be adopted. The Company will Process Sensitive Personal Data if:

3.2.1 The Data Subject has given his or her explicit Consent to the Processing or

3.2.2 The Processing is Necessary for the purposes of performing obligations or exercising specific rights under employment and social security and social protection law; or

3.2.3. The Sensitive Personal Data has been deliberately made public by the Data Subject; or

3.2.4. The Processing is in accordance with the Law or is necessary to protect the Data Subject's (or another person's) "vital interests" (or those of another person) and the Data Subject is physically or legally incapable of giving Consent;

4. INFORMATION

4.1 The Company informs the Data Subjects about the processing of their data. The information takes place prior to the commencement of the Processing of their Personal Data

(or if at a later date, as soon as possible) from the moment this Policy is activated). The information is provided in a written, concise, transparent, understandable and easily accessible form, using simple uncomplicatedlanguate.

4.2 The following is noted:

4.2.1 The Data Subjects having an employment relationship with the Company have been informed of the Processing of their Personal Data from the company, as well as of their right of access to their Personal Data, or the right of filing a complaint with the Data Protection Authority. They are also informed for any possible new processing system added or replacing the previous, to the extent the kind, or extent of the processing changes.

4.2.2. The Company collects personal data of its employees directly from same. In case of data collection from third parties, then the employees will need to be informed, unless this is obvious to them. Similarly, the employees are to be informed when the processing of Personal Data becomes totally voluntary and not in performance of the purpose of the employment relationship.

4.2.3. For the information of any third party (ie clients, suppliers, visitors) non employees of the Company, the Company maintains in its website a relevant post, containing information for the processing of non sensitive Personal Data.

4.2.4. In case a Data Subject requests information for the processing of his/her personal data from the Company, the Company maintains the right to deny providing said information in the cases provided for in the Law, or in case no notification if required by the Law.

5. CONSENT

5.1. When basis for the processing of Personal Data is the consent of the Data Subject (ie due to processing of personal data, or transfer of data outside the EU) a clear, freely given consent of the Data Subject is required, following his/her relevant information, by a statement or a clear affirmative action (such as ticking a box), signifies agreement to the Processing of his or her Personal Data. Mere failure to respond does not amount to Consent.

5.2 Consent may be withdrawn at any time. Consent is not basis for the processing of employee Personal Data, unless the Processing is totally voluntary. As a rule, basis for the lawful Processing of Personal Data for HR purposes shall be the fulfilment of an obligation arising from the law, the performance of a contract, the lawful management of Human Resources and should not be the Data Subject's Consent.

5.3 Explicit consent shall be requr3ed when the purpose of the Collection and Processing are Sensitive Personal Data, unless there is no alternative legal basis.

5.3.1. Consent should be requested in an intelligible and easily accessible form, using clear and plain language, making sure that the Data Subject understands that he or she is free to grant the requested consent without suffering any adverse consequence, and that the Consent can be withdrawn at any time, with information as to a straightforward way;

5.3.2.if the Consent is obtained in written form, and the relevant document also concerns other matters, make sure that the Consent is clearly distinguishable from the other matters; and

5.3.3. Make sure that Company has an appropriate record of the Consent having been given.

5.4. Where explicit Consent is required, Company will provide to the Subject all the information required by the Regulation in ARTICLE 13, also set out in Annex 1, and the Data Subject will then need to make an explicit written statement (or expressly agree to an explicit statement provided by Company) agreeing that the Processing may proceed.

5.5. Company will confirm that the principles set forth hereinabove have been observed in every case International Transfer of Personal Data .

6. DATA PRESERVATION AND DESTRUCTION

The Company needs to know, and in certain instances defined by the law, is obliged to maintain record of the processing activities. The Record of Processing shall contain the elements mentioned in Annex 2.

The Company shall delete or anonymize or limit/interrupt the processing of Personal Data when there is no longer need, according to the applicable law, or the relevant retention policy of the Company. If files containing Personal Data are kept according to the applicable law and the present policy, the employees responsible for said data shall have to regularly control them and delete Personal Data (or files which contain them) which are no longer necessary deleting e-mail addresses from electronic correspondence files.

7. DATA SECURITY AND THIRD PARTY CONTRACTS

7.1. The Company will have technical and organisational security measures in place to protect all Personal Data that it Processes in accordance with its security policies.

7.2. Where Company outsources the Processing of Personal Data to any third party service provider it will:

7.2.1. conduct appropriate due diligence on the technical and organisational security arrangements that the service provider will have in place to protect those Personal Data;

7.2.2 ensure that the arrangement is governed by a written agreement imposing obligations on the service provider according to the present Policy; and

7.2.3 take reasonable steps (for example by exercising audit rights and/or making enquiries of the service provider) to ensure that the security measures required of the service provider are in place in practice over time during the life of the relevant Processing arrangement.

7.3 The contracts with third parties service providers contain special terms, including audit rights.

7.4 The Company is obliged to report certain breaches of security affecting Personal Data to competent data protection authorities, and in some circumstances it is obliged to inform affected Data Subjects. An employee who becomes aware of or suspects such a breach should report the breach to the Data Protection Coordinator, so that the Company can comply with its legal obligations and, generally, investigate and respond to the apparent breach.

For the matters of video surveilance, the terms of Annex 3 hereto shall apply.

8 DATA SUBJECTS' RIGHTS

8.1. Data Subjects have the right:

8.1.1 to be provided with a copy of any Personal Data that Company holds about them, with certain related information;

8.1.2 to require Company, without undue delay, to update or correct any inaccurate Personal Data, or complete any incomplete Personal Data, concerning them;

8.1.3 to require Company to stop processing their Personal Data for direct marketing Purposes; and

8.1.4. to object to the processing of their Personal Data more generally.

8.2. Data Subjects may also have legal rights, including in certain circumstances:

8.2.1 to require Company, without undue delay, to delete their Personal Data;

8.2.2 to temporarily or permanently "restrict" (i.e. suspend) Company's Processing of their Personal Data, so that it can only continue subject to very tight restrictions; and

8.2.3 to require Personal Data which they have provided to Company, and which are Processed based on their Consent or during the performance of a contract with them, to be "accessible" to them or an alternative service provider.

If Company receives a communication from any Data Subject by which he or she seeks to exercise any of these rights, said communication should be handled in accordance with the specific Subject Access Request Pcess.

9. AUTOMATIC RESOLUTION- MEASURES (INCLUDING PROFILING) INTERNATIONAL DATA TRANSFER

9.1 Company will only Transfer Personal Data outside the European Region:

9.1.1 where the Transfer is to a country or other territory which has been assessed by the European Commission (or an equivalent UK body) as ensuring an adequate level of protection for Personal Data

9.1.2 where the Data Subjects have given their explicit Consent to the Transfer taking place; or

9.1.3 where the Transfer is in accordance with the law.

The Company shall not proceed to an automated Personal Data Processing in order toadopt resolution which create legal consequences concerning Data Subjects, exclusively from the mentioned automated processiong, save under the terms and conditions of the GDPR and other applicable laws.

10. OBLIGATION TO OBSERVE THE PRESENT POLICY

All the natural or legal persons processing Personal Data for the account and in the Name of the Company, including its partners and employees, must abide by this policy and report any existing or possible breach thereof to the Data Protection Coordinator of the Company. Non compliance with the present policy constitutes a serious breach which entails all kinds of legal consequences (including dismissal).

In parallel every employee and every department head of the company informs the Companys' Data Protection Coordinator about any new processing of Personal Data, in order for the Processing Records to always be updated.

11. THE DATA PROTECTION COORDINATOR

The Company has appointed a data protection coordinator (Data Protection Coordinator) in order to oversee the observance of the Regulation and to answer any questions/requests/complaints of Data Subjects.

The Data Protection Coordinator may keep also all files needed for the proof of the company's compliance with the Regulation (Archive edits, conset forms, recording Data Subject's Request, etc)

12. CO-OPERATION WITH DATA PROTECTION AUTHORITIES

The Company is obliged to co-operate with the competent data protection Authority in the performance of its tasks. Any communication received from a competent data protection authority should be passed to the Data Protection Coordinator as soon as is reasonably practicable.

ANNEX 1
INFORMATION TO BE PROVIDED TO DATA SUBJECTS

According to Article 13 of the Regulation, the information referred to in this Policy is:

1. the identity and contact details of the Company's representatives controlling the Processing of the relevant Personal Data;

2. the contact details of the Data Protection Coordinator, or the Data Protection Officer, of the Company

3. the purposes for which the Company intends to Process the Personal Data;

4. the legal basis for the Processing (for example, the Legitimate Interests, consent);

5. where the Processing is justified on the basis of the Legitimate Interests Condition, the relevant legitimate interests pursued by Company or another person which Company relies upon to justify the Processing;

6. where Company is not collecting the Personal Data directly from the Data Subject but from a third party, the categories of Personal Data collected and the sources from which they are collected ;

7. any intended recipients or categories of recipient of the Personal Data (this means recipients outside Company, such as third party service providers);

8. where applicable, the fact that Company intends to Transfer the Personal Data to a country or territory outside the European Region, together with information as to:

8.1.1 whether the relevant country has been determined by the European Commission to ensure an adequate level of protection for Personal Data; and

8.2 where this is not the case, and if Company justifies Transferring the Personal Data to that country or territory on the basis that it has put in place adequate safeguards to protect the Transferred Personal Data (for example, an appropriate data transfer agreement), the nature of those safeguards and that a copy can be obtained from the Data Protection Coordinator;

9. the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

10. the existence of the legal right to request from Company access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subjects or to object to Processing as well as the right to data portability, and that these rights can be exercised by contacting the Data Protection Coordinator or the Data Protection Officer;

11. that the Data Subjects can, if they so wish, lodge a complaint about Company's Processing of his or her Personal Data with the competent data protection authority;

12. where Company is collecting the Personal Data directly from the Data Subjects, whether provision of the requested Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide it; and

13. detailed information about any automated decision-taking techniques that may be used and, where applicable, the rights of the individuals to object the adoption of any automatic decision affecting them.*

ANNEX 2
DATA PROCESSING RECORDS AND FILINGS

A. Processing Records

1. The Company keeps record of all the processing activities under its responsibility. Said file contains the following information:

a. the name, or title and the communication data of the Controller and as the case may be any joint Controllers and Controller,

b. the scope of the processing

c. the categories of recipients to whom are notified or are going to be notified personal data, including recipients in third countries or international organizations

d. description of the data subject categories and the categories of personal data

e. where applicable the use of profiling

f. where applicable, the categories of personal data transfers to a third country of international organization

g. mention of the legal basis of the processing, including the transfers for which the personal data are intended

h. if possible, the deadline for deletion of the various personal data categories

i. if possible a general description of technical and organizational safety measures adopted by the Company for observing the law.

2. The Company keeps record of all categories of processing activities undertaken by same or through third parties processors which includes the following:

a. name and contact details of the data processor/s, any controller on behalf of which the data processor operates and as the case may be the data protection officer

b. the categories of processing performed for the account of any controller

c. as the case may be, the personal data transfers to third country or international organization, including definition of said third country or international organization, as longas express mandate from the controller has been given

d. if possible a general description of the technical and organizational measures adopted by the company

3. The files mentioned i n paragraphs 1 and 2 exist in writing u.a. in electronic form.

B. Filings

1. The controller and the processor keep record at least for the following acts of processing in the systems of automated processing: collection, transformation, information research, communication, including transfers, combination and deletion.

2. The record keeping of information research and disclosure thereof should take place in a way, in order to render possible the determination of the justification, date and time the acts mentioned in par. 1 took place and to the extent feasible, identify the persons who participate therein and specifically the person who sought information or disclosed personal data, as well as the identity of recipients of the mentioned personal data.

3. The controller takes into account the requirements of paragraphs1 and 2 already during the planning of procedures and corresponding systems and processes.

4. Subject to procedural rules said filings may be used exclusively for the verification of the legality of the processing, the exercise of internal audit by the controller or the processor, the safekeeping of the integrity and security of the personal data, as well as in the framework of criminal procedures.

5. The controller and the processor set the records at the disposal of the supervising authority, upon request.

ANNEX 3

RULES FOR VIDEO SURVEILANCE

Systems permanently placed in a space, operating constantly or in regular intervals having the possibility to capture and/or transmit sound and/or image signal from said space to a specific number of projection monitors and/or recording devices by the company of for its account, are regulated by the below rules.

1. The data should not be kept for a time period longer than the one required for the intended scope. Upon condition that no incident results from the reception of sound and image data store or received in real time, the data should be destroyed latest within fifteen (15) calendar days, notwithstanding any special dispositions of the applicable laws for the specific categories of controllers. In case of an occurrence regarding the scope of the processing, it is permissible for the Company to keep the data in a separate file for three (3) months. After expiration of the above time period, the Company may maintain the data for a longer specific time period only in exceptional cases where the occurrence requires further investigation. In such a case the Company has the obligation to inform the Authority for the required time frame for such record keeping.

2. The transfer to third parties of data deriving from the video surveillance system is permissible in the following cases:

a. following prior consent of the data subject.

b. exceptionally the transfer is permitted also without consent after a dully justified third party request, when the data are needed to be used as evidence for the proof, exercise or support of legal claims, or a punishable act and may contribute to the investigation of facts or the identification of perpetrators. The transfer of personal data to the competent judicial, DA and police authorities, which the latter request during the performance of their duties, shall not be considered a transfer to a third party.

3. The Company is obliged to maintain the appropriate organizational and technical measures for the confidentiality and safety of said data as well as their protection from any form of illegal or unlawful processing, such as access control or safe transmission.

4. Before any person enters in the range of the video surveillance system, the Company is obliged to inform it, in the most appropriate, apparent and understandable way, that it is about to enter into a space where a CCTV system is in operation, the nature of the system used, the spaces of installation and the range, as well as the time period for keeping the data.

5. Subject to the dispositions of article 15 of the Regulation, when the right of access of the data subject is exercised on image and sound data kept by the controller, - he has an obligation to provide within fifteen (15) days from submission of the relevant request a copy of the portion of the registered image where the data subject has been recorded, or the printed sequence of the recorded pictures or proportionally inform the interested party in writing within the same deadline, either that it is not appearing or that the specific part of the recording is no longer kept. Alternatively, if the data subject agrees to it, the Company may simply directly show the above section. For this purpose the data subject is obliged to indicate the exact time and place when it found itself in the camera range.

6. When the Company provides a copy of images, it should scramble the images of third persons by any appropriate technical means, if it is possible to breach their right to privacy, unless it is a simple demonstration.

7. The data collected through CCTV may not be used as exclusive criteria for the evaluation and employee productivity

8. Transfer of the video surveilance data outside the EU may take place only subject to the dispositions of the law.