BINDING CORPORATE RULES ON PERSONAL DATA PROTECTION

TOR HOTEL GROUP

1. Purpose

1.1. Legal nature of binding corporate rules

BCRs are policies in relation to the processing of personal data enforced by all companies of Tor Hotel Group with legally binding effect.

2. Scope of provisions

This present Policy applies for "A.E. MAKEDONIKON XENODOCHEION ", Business Registry 123042204000, having its seat in Thessaloniki, 11, Komninon street , VAT no. 094009344, Tax Office FAE THESSALONIKIS, legally represented (hereinafter called the "Company") and "TOURISTIKES EPICHIRISEIS HALKIDIKIS A.E ", Business Registry Number 122622004000, having its seat in Thessaloniki, 11, Komninon street, VAT no. 094052101, Tax Office FAE THESSALONIKIS, legally represented (hereinafter called the "Company").

BCRs apply to any kind of processing operations on all types of personal data within Tor Hotel Group, irrespective of where the data are collected. Personal data are being processed by the Group mainly for the following purposes:

Management of employees' data when entering into a contract and provision of products and services offered to employees by the Group or third parties.

Initiation, implementation and processing of contracts with corporate clients, as well as direct marketing purposes in order customers and interested third parties to become aware of the products and services offered by the Group or third parties.

Contracting and implementing agreements with service providers towards the Group as part of provision of services.

Contracting agreements with other third parties, mainly shareholders, associates or visitors, and compliance with legal binding effect.

Personal data are being processed to serve purposes – current or future- within Tor Hotel Group, which include the provision of hotel and tourism services, as described in the articles of association of the Group's companies.

Transfers of data within affiliated companies of the Group which are necessary for management , processing operations and business continuity.

In pursuit of the Group's legitimate interests, to record CCTV footage to ensure the safety and security of premises, staff and customers;

3. Relation with other legal provisions

Provisions aim to achieve a high level of protection of personal data within Tor Hotel Group. Therefore, regulations, procedures etc, which apply in the companies of the Group and override the principles predicted from BCRs or impose additional restrictions during processing of personal data, continue to be enforceable as it be.

Enforcement of European or national legislation, including mainly legislation concerning public security, defence, national security and criminal law, which requires transmission of data to third parties, is not being affected by the policies of BCRs. If a company ascertains that policies of BCRs violate the general data protection regulation or national law on personal data then the controller or every company of the Group is immediately informed.

4. Expiration and termination

BCRs cease to be binding for a company if that company leaves the Group or terminates the contract. However, expiration or termination of BCRs does not exempt the company from its legal obligations in relation to the data that have already been transmitted. Furthermore transfer of personal data from or to the company can only take place if other procedural guarantees are provided in accordance with the requirements of European legislation.

5. Publicity

This policy is published on the webpage of each Company and is freely accessible by all employees, associates and clients. The companies of the Group provide any information, concerning the rights of the data subjects. This information becomes available to the public in a plain language.

6. Transparency in data processing

The right to be informed

Data subjects are being informed in relation to the processing of their personal data in accordance with current legislation and the following terms:

The company informs efficiently the data subjects for the following:

- The identity of the controller or processor (or controllers or processors) and his (their) contact information.
- The purpose for which personal data have been collected and the intended further processing, specifically which data might be disclosed and / or are being subject to

processing / or are being processed, for which intended purpose and for what period of time.

- If personal data are transferred in third parties, the subject of the data is being fully aware about the recipient, the range and the purpose of transfer.
- The rights of the subject in relation to the processing of his personal data.

Regardless of the means of providing the information, the relevant information shall be addressed to the data subject in plain language.

The information is made available to data subjects, from the moment that the data have been collected and afterwards, whenever it's requested.

7. Processing of personal data

Personal data are processed only under the following terms and shall not be processed for purposes other than those for which were originally collected**.**

Processing of the collected data for different purposes is allowed only if:

- current legislation allows processing of personal data for the specified purpose;
- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation of the company's;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the company or by a third party, provided that the interests of the data subject's clearly do not outweigh the interests of the company's.

8. Common rules applicable to processing and transmissions within the Group.

8.1. With regards to processing and transmissions of personal data as described in the present, companies of the Group and its employees agree to abide by the following rules.

Limitation of purpose:

- personal data as in detail are listed at the Annex will be processed and transferred within the companies of the Group for specified, explicit and legitimate purposes, in

accordance with the objectives set out in the Annex. Personal Data that have been processed and transferred will not in any way subject in further processing incompatible with the initial purposes.

- Companies of the Group will limit processing of personal data listed in detail in the Annex only in what is necessary taking into consideration the intended purpose/-s.

- Companies of the Group will use adequate means in order personal data to be kept accurate, complete, up to date and reliable for their intended use.

- Companies of the Group will store personal data only for as long as is required to meet lawful business purposes for which personal data were collected and in compliance with the storage policies of the affiliated companies, unless if it is otherwise required by applicable law or provisions.

- Products and services shall be provided only under the terms agreed prior entering into the contract, the data subject shall consent to the processing of his personal data only for these purposes.

9. Lawfulness for processing of personal data:

Processing of personal data shall be based on at least one of the following lawfulbases:

- explicit consent of the data subject;

- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior entering into a contract;

- processing is necessary for compliance with a legal obligation to which the company is subject;

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or a third party to whom personal data have been or will be disclosed;

- processing is necessary for the purposes of the legitimate interests pursued by the Group, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

10. Consent of the data subject

The data subject shall consent if:

- Consent has been given by a clear affirmative act, voluntarily and after informing the subject, in such a way that the data subject becomes aware about the purpose of his consent. The declaration of consent is accurate and informs the data subjects for their right to withdraw consent without detriment. In the event that the withdrawal of consent implies the non-fulfillment of the contractual obligations, the data subject must be informed.
- Consent has been received in an appropriate form for the occasion (written). In exceptional cases, verbal consent may also be obtained, if that is adequately recorded, as well as the special circumstances that make verbal consent sufficient.

11. Automated use of personal data

Decisions evaluating personal aspects of a natural person and which produces legal effects concerning him or her or similarly significantly affects him or her shall not be based solely on automatic processing of personal data. This includes, in particular, decisions in relation to reliability, natural performance at work or health status of the data subject.

If, in individual cases, there is a need for automated use of personal data, the data subject shall be informed with no further delay about the result of the automatic processing, and should be given the opportunity to submit his observations within a reasonable time period. Any comments of the data subject shall be taken into consideration before the final decision.

12. Use of personal data to promote products/ services

In the event that data are being used in order to promote products/ services, the data subjects should:

- be informed in relation to the way that data are processed for promoting products/services;
- be informed for the right to refuse processing of their data for these purposes;
- be given adequate information to exercise this right. Specifically, shall be informed about his/her right to lodge a complaint against the company processing his/her personal data.

13. Processing of special categories of personal data (sensitive data)

The use of special categories of personal data is allowed solely if that is predicted from current legislation or if data subject has given explicit consent. In additional, processing is allowed in the event that is necessary for fulfillment of legal obligations, arising from employment law, under the condition that it is allowed by national law and appropriate measures for their protection have been received.

Prior to storage and processing of sensitive data, the company informs the controller. When evaluating the conditions under which processing of personal data is lawful, special attention shall be given to the nature, scope, intended purpose, necessity and lawfulness of processing of sensitive data.

14. Lawfulness for the processing of sensitive data:

Processing of sensitive data is based on at least one of the following lawful bases:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of each company's of the Group in the field of employment and social security and social protection law in so far as it is authorized by National Law or Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights;

- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

- processing relates to personal data which are manifestly made public by the data subject;

- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional, and subject to the conditions and safeguards of national law or legislation laid down by national competent bodies, in particular the obligation of professional secrecy or by another person who is also subject to a corresponding obligation of confidentiality, or

- processing of sensitive data is necessary for reasons of substantial public interest provided either by national law or by decision of the supervisory authority.

- For reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health.

15. Limited access to Personal Data

Processing of personal data should be limited only to those employees of each affiliated company whose work/-s and responsibility/-ies make this necessary.

16. Data minimization, data avoidance, use of anonymous and pseudonymous data

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization). The data are processed only in the information systems that are necessary to fulfill that purpose (data avoidance).

When it is feasible and financially reasonable, should be taken all objective factors for erasure of personally identified or identifiable information of data subjects' (anonymization) or their replacement with other characteristics (pseudonymisation).

17. Transmission of personal data

17.1 Nature and purpose of transmission of personal data

Personal data are transferred only if the recipient of the data assumes responsibility for the data received or when the recipient uses data exclusively in accordance with the sender's guidelines and requirements (data processing agreement).

Personal data are allowed to be transferred only for the described purposes in the context of business activities or due to a legal obligation or after consent of the data subject.

17.2 Transfers of data to third countries

Any processing of personal data shall take place exclusively within the territorial boundaries of a Member-State in the European Union (E.U.) or another (State) which has signed the Treaty on the European Economic Area (EEA). Transfers of data in a third country require written consent of the data subject and are subject to compliance with the specific conditions set out in Chapter 5 of the GDPR.

When transferring personal data to a third party, are applied appropriate technical and organizational measures for their protection based on the requirements of the Group.

18. Processing of personal data from controllers outside the group of companies and subcontracting

When a company of the group assigns to a third party (processor) the provision of services on its behalf and in accordance with its instructions, then in addition to the contract of services which defines the type of the provided service, the contract shall refer to the obligations regarding the processing of personal data undertaken. These obligations shall include instructions on the type and way of processing of personal data, purpose of processing and technical and organizational measures that are required for their protection.

Controller shall not use personal data (which have been transferred for entering into a contract) for his/hers purposes or third parties, without prior consent of the company's.

Controller shall inform the company in advance in case that wishes to use subcontractors, in order to fulfill its legal obligations. Every company of the Group must have the right to refuse the use of subcontractors. In case of subcontracting, processor carries responsibility for his subcontractor in order to comply with the requirements, arising from the contract between the processor and each company's of the Group.

Processors should be selected on the basis of their ability to fulfill the above mentioned requirements.

19. Security and confidentiality

Personal data shall be correct and, where necessary, kept up to date.

In the light of the purpose for which data are being processed, appropriate measures shall be taken to ensure that any incorrect or incomplete information is erased, blocked, if it is deemed necessary, corrected.

20. Security of personal data – Technical and organizational measures

Each company adopts appropriate technical and organizational security measures and applies them to the personal data processing systems and platforms whichare used for storage, processing or use of the personal data.

Such measures shall include:

- preventing unauthorized persons from gaining access to data processing systems. (admittance control);
- ensuring that data processing systems cannot be used by unauthorized persons (denial-of-use-control);

- ensuring that those persons authorized to use a data processing system are able to access exclusively the data to which have authorized access and personal data cannot during processing be read, copied, altered or removed by unauthorized persons (data access control);
- ensuring that, in the course of electronic transmission or during its transport or recording on data media, personal data cannot be read, copied, altered or removed by unauthorized persons, and that is possible to check and identify the controllers to which personal data are to be transmitted by data transmission equipment (data transmission control),
- ensuring that is possible retrospectively to examine and establish whether and by whom personal data have been entered into data processing systems, altered or removed (data entry control),
- ensuring that outsourced personal data can only be processed in accordance with the instructions of the customer (contractor control);
- ensuring that personal data is protected against accidental destruction or loss (availability control);
- ensuring that data which have been collected for different purposes can be processed separately (separation rule).

21. Rights of the Subject

21.1. Right to be informed

Data subjects shall have the right to obtain from any company processing their personal data confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period as well any available information as to their source;
- the purposes of the processing;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- policies of present BCRs.

All information should be made available to the applicant in a plain language and within a reasonable time framework. This is in generally achieved by printed or electronic communication. Providing a copy of BCRs to the applicant is considered to be sufficient information in relation to the demands set out from this agreement.

21.2 Right to object, right to erasure or right to restriction of processing/ right of correction and right to lodge a complaint with the competent supervisory authority.

The data subject shall have the right to object, on grounds relating to his or her personal situation, at any time to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

The right of objection continues to apply even if the subject might have given his/her explicit consent in a previous occasion for processing of his/her data.

Legal requests to erase personal data or restrict processing must be met immediately. Specifically, as lawful are considered requests for erasure of data when there is no other legal ground for the processing. If the data subject has the right to erasure, but such an erasure is not possible, personal data shall be protected from unauthorized use by restricting access. The storage period of personal data, provided by national legislation, must be observed.

The data subjects shall have the right to obtain from the company which storages without undue delay the rectification of inaccurate personal data concerning him or her at any time, in the case that those are incomplete or / and inaccurate.

The data subject is informed in the case that revocation of his consent or erasure of personal data results to a void contract.

The data subject has the right to lodge a complaint against any of the companies of the Group if considers that a company of the Group does not processing his personal data in accordance with the legislation or policies of BCRs. Documented complaints will be examined into a reasonable time framework and the data subject will be informed.

If a complaint concerns more than one companies of the Group, the controller company, who has dealt with the complaint, takes over all relevant communication with the data subject.

Appropriate communication channels should be available for reporting personal data incidents (e.g. e-mail account).

For the competentauthority and the way of lodging a complaint, you can visit the following website (www.dpa.gr)

21.3. How to exercise the rights of subjects

The data subjects will not face any discrimination due to the fact that they have exercised the above mentioned rights. The way of communication with the data subject, e.g. by

telephone, electronically or in writing, shall be chosen, where possible, upon the request of the data subject.

21.4. Copy of BCRs

Copy of BCRs must be made available in written form to anyone requested.

22.Administrative organization

22.1. Responsibility for data processing

Companies are required to ensure compliance with data protection legislation and with present BCRs.

22.2. Data protection officer

Each affiliated company shall appoint an independent, data protection officer whose duty is to ensure that the individual organizational units of the company are advised on the statutory and internal requirements of Tor Hotel Group for data protection and, in particular, on these Binding Corporate Rules. The data protection officer shall use suitable measures, in particular random inspections, to monitor compliance with data protection regulations.

Each affiliated company shall ensure that the data protection officer possesses the relevant expertise for evaluating the legal, technical and organizational aspects of data privacy measures.

Each affiliated company shall provide the data protection officer with the financial and personnel resources required for carrying out his/her duties.

The data protection officer shall be granted the right to report directly to company management and shall be connected organizationally to company's management.

The data protection officer shall be responsible for implementing the requirements of Tor Hotel Group / all affiliated companies and data privacy strategy.

All departments of each company shall be obliged to inform their company's data protection officer of any developments in IT infrastructure, network infrastructure, business models, products, staff data processing and corresponding strategic plans. The data protection officer shall be brought in on new developments at an early stage in order to ensure that any data protection matters can be considered and evaluated.

22. Internal procedures for handling complaints

Any data subject who considers that his/her personal data in the Annex might have been processed in breach of these BCRs by any legal entity of the Group may submit his/hers queries and complaints to the data protection officer at mail: privacy@torhotelgroup.gr.

Any employee of the Group who believes that his / her personal data may have been improperly processed can either contact the human resources department or the data protection officer at the e-mail address: privacy@torhotelgroup.gr.

Apart from exceptional circumstances, controller will send confirmation of receipt of the complaint to the complainant within five (5) working days.

DPO will investigate and contact colleagues from the departments concerned, as required to deal with the complaint and provide a substantive response to the complainant without undue delay and in any event within one (1) month of receipt of the request.

If due to the complexity of the complainant DPO is unable to provide a substantive response within one (1) month, will inform the complainant and will provide a reasonable estimation (not exceeding two [2] months) within the time framework in which shall be answered.

If the complaint is legally sound, DPO will ensure all necessary steps are taken,in accordance with applicable laws.

Additional reporting obligations for the employees:

Any employee of the Group who has reasonable reasons to consider that these BCRs have been breached will have to contact his supervisor, the human resources department or the data protection officer at privacy@torhotelgroup.gr.

Irrespective of the internal procedures for handling complaints, the data subjects should have the right at all times to seek advice and lodge a complaint to the competent authority or/and to file a claim to the competent court.

23. Duty to Inform in case of breach

Company must immediately inform the data protection officer for any breach or clear indication of breach of data protection regulations and mainly the current BCRs, especially in cases where the incident may have an impact on the public or/and affects more than one companies of the Group or/and results economic loss.

24. Employee commitment and training

Companies shall ensure that employees keep confidentiality of personal data and confidentiality of telecommunications when entering into the employment contract.

Employees shall receive sufficient training on personal data matters. Each company shall establish such procedures and provide essential resources for these purposes.

Employees shall receive training in relation to the basic principles of personal data at least every two years. The company shall provide special training programs. The data protection officer of each company shall keep records of all trainings that have taken place and shall inform the data protection officer of the Group on an annual basis.

The Group's data protection officer may allocate resources and procedures centrally for training the Group's employees.

25. Cooperation with the supervisory authority

Companies shall cooperate, on request, with the supervisory authority to which they belong or with the competent authority to which the company that transfers the data belongs and in particular must answer its queries and follow its recommendations.

26. Contact person for queries

The Data Protection Officer of each Company of the Group is responsible for handling queries related to BCRs. Communication with the data protection officer of the Group is done during working hours in the following ways:

E-mail: privacy@torhotelgroup.gr.

Adress: Komninon no. 11, Thessaloniki, Zip Code 54624

Phone numbers: +30 2310 269421, +30 2310 021 020

27. LIABILITY

28.1. Scope of liability provisions

This chapter applies exclusively to the processing of personal data collected in the EU / EEA and falls within the scope of the GDPR (Regulation 2016/679 EU) for personal data protection and national law.

28.2. Compensation

Any person who has suffered material or non-material damage as a result of an infringement of this regulation shall have the right to receive compensation from the companies of the Group for the damage suffered.

In the event that a company of the Group paid full compensation for the damage suffered, has the right to raise an action of recovery against the company which is responsible for the damages or is related to the third party, who caused it.

The data subject is entitled to bring a claim for compensation initially against the company that transferred the data. If the company is not liable de jure or de facto (under applicable legislation or facts), the data subject has the right to claim compensation from the company that received the data. Company – recipient in case of breach is not entitled to limit its liability referring the contractor's liability.

The data subject has the right to lodge a complaint to the competent supervisory authority or to the supervisory authority which at that moment is competent.

28.3. Burden of Proof

The burden of proof regarding accurate processing of personal data of the data subject lies with the responsible company.

28. Competence of Courts

The data subject may choose to claim compensation before the competent Greek courts.

Alternative, if the data Subject has its usual residence in an EU Member State or the EEA, the courts of that State shall also have jurisdiction.

The right of the data subject to file a claim under the competent supervisory authority or to apply to the competent courts is not being affected by the above described procedure.

29. FINAL PROVISIONS

30.1. Amendment

Data protection officer of each company of the Group reviews the BCRs regularly and at least once a year, in order to harmonize them with the current legislation and make all necessary amendments.

Data protection officers of the companies' are required to review whether BCRs amendments affect the legal obligation of compliance with current legislation or whether contradict national legislation.

30.2. Procedural issues / Severability clause

If individual provisions of BCRs are or become void, these should be deemed to have been replaced by other policies, which are as close as possible to the main meaning of the BCRs and the void provisions. In cases of doubt or in the absence of relevant provisions the current legislation of the European Union on personal data applies.

For « A.E. MAKEDONIKON XENODOCHEION »	For « TOURISTIKES EPICHIRISEIS HALKIDIKIS A.E »
Date:	Date:

ANNEX

TRANSMISSIONS BETWEEN AFFILIATED COMPANIES

Categories of personal data:

Data of the companies' employees:

Concerns employees in each affiliated company of the Group (including the former employees), as well as candidates who apply for a job position or send their CV to meet future needs in human resources. Finally, data on relatives of employees may be requested (e.g. spouse, children).

Related information: contact information (e.g. full name, home and work addresses/ telephone numbers / e-mails, business fax numbers, emergency contact details), identity card or passport details, personal details (e.g. gender, date of birth, place of birth, marital status, family composition, nationality), social security number, educational level, length of service, areas of specialization, professional details (e.g. job title, work position), employee performance, salary, allowances, compensation, information related to payments (e.g. bank account number), photographs, visual records, criminal record, health certificate, medical advice on illness, income tax return.

Data of external associates and suppliers (and any of their representatives / employees):

It concerns associates, who are not employees in any of the companies of the Group but provide services under a contract or similar agreement to one of the affiliated companies.

Related data: contact details (e.g. full name, business address, telephone and fax numbers, e-mail addresses), payment information (including bank account information), VAT number and other invoicing information

Customer Data:

Concerns customers of each Company's of the Group as well as the consumers to whom services/ products are addressed.

Related information: contact details (e.g. full name, home and work addresses / telephone / e-mail addresses, fax numbers, emergency contact details), identity card or passport details, personal details (e.g. gender, date of birth , place of birth, marital status, family composition, nationality), information related to payments (e.g. bank account number, credit card number), health data for use of spas / wellbeing centers, vehicle registration number, visual records, customer interaction data (e.g. a. usage behavior: website visits, click tracking, call logging, b. social media activity: posts, likes, comments, c. survey response data, d.

feedback), location data, lifestyle (e.g. interests, tastes, hobbies, preferences: music, sports, food, movies).

For « A.E. MAKEDONIKON XENODOCHEION»	For « TOURISTIKES EPICHIRISEIS HALKIDIKIS A.E »
Date:	Date: