2018

Privacy Policy

version 1.0.

GDPR compliant

Hajdúszoboszló

Thermal Hotel Garden

2019.01.01.

Privacy policy

PINTAKOL KFT.
4200 Hajdúszoboszló Debreceni út 6.
Tel: +36 52/ 557-550, e-mail: thermalhotelgarden@gmail.com

.....
Szilárd Pintácsi
Managing
Director

Purpose of the rules:	Full establishment and regulation of the company's data management and full information to data subjects
Scope of the Rules:	PINTAKOL KFT.
Subjects of the Regulation:	all partners, customers and employees
Status of the regulation:	Published / in force
Version number:	001
Date of entry into force:	2019.01.01.
Date of repeal:	
Approval:	Managing Director
Access Rights:	Public

Content

I. GENERAL PROVISIONS - PREAMBLE

1. THE PURPOSE OF THE POLICY

The aim of PINTAKOL LTD is to ensure an adequate level of protection of personal data in its processes and procedures that involve the processing of personal data in the context of its activities, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) 95/46/EC (General Data Protection Regulation or the Regulation).

The purpose of the Rules is to define the internal provisions that ensure the legal compliance of the operation of the records kept by the Data Controller, the compliance with the constitutional principles of data protection, Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: **Infotv.**) and other legal requirements of data security, and to prevent unauthorized access, alteration and unauthorized disclosure of data.

In accordance with the operation of the Data Controller, in particular in relation to the Data Controller's contracted service providers, employees and customers, data processing issues arising from the performance of financial services and ancillary financial services activities shall be treated as a priority.
The purpose of this Policy is to inform the employees, agents, system users and customers of the Controller of the rules and procedures applicable to the processing of personal data.

The Controller shall design and implement the processing operations in such a way as to ensure that the privacy of the data subjects is adequately protected. It shall take the technical and organisational measures and establish the procedural rules necessary to ensure data security, taking into account the state of the art. In particular, it shall protect data against unauthorised access, alteration, disclosure, transmission, disclosure, deletion or destruction, accidental destruction or accidental loss, damage or loss of data and inaccessibility resulting from changes in the technology used.

Where the Data Controller uses a data processor, the Data Controller shall ensure that the selected data processor takes the necessary measures to protect personal data and follows the policies and specific instructions of the Data Controller. When selecting a processor, the Controller shall endeavour to use only a processor which offers adequate guarantees, in particular as regards its expertise, reliability and resources, to implement technical and organisational measures to ensure compliance with data protection requirements, including security of processing.

2. THE DATA CONTROLLER

Company name:	Pintakol Kft.
Seat:	4200 Hajdúszoboszló, Debreceni út 6.
Main activity:	Restaurant, mobile catering Company
registration number:	09-09-030548
Tax number:	26143037-2-09
Statistical number sign:	26143037-5610-113-09

3. THE SCOPE OF THE RULES

The scope of the Policy covers all processing of personal data by the Controller.

4. THE SUBJECT MATTER OF THESE RULES

This Policy applies to all employees of the Data Controller, individuals in other employment relationships, all partners of the Data Controller or natural persons who come into contact with the Data Controller through a partner, all persons who come into contact with the Data Controller by contract or offer, and all employees of external organisations who use, operate, manage or develop the Data Controller's IT systems, i.e. who have access to the Data Controller's data assets.

5. RELEVANT LEGISLATION

- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information
- Data Protection Regulation

II. <u>DEFINITIONS</u>

1. **'controller'** means a natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of the processing are determined by Union or Member State law, the controller or specific criteria for the designation of the controller may also be determined by Union or Member State law;

2. **"personal data" means** any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

3. **"processing" means** any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

4. **"transfer"**: where the data are made available to a specified third party (in particular: a data controller discipline, company or authority other than the customer's original purpose).

5. **"processing" means** the performance of technical tasks related to processing operations, irrespective of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data.

6. **"restriction of processing" means** the marking of stored personal data for the purpose of restricting their future processing;

7. **"profiling" means** any form of automated processing of personal data whereby personal data are used to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict characteristics associated with that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

8. **"processor" means a** natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

9. **"recipient" means a** natural or legal person, public authority, agency or any other body to whom or with which personal data are disclosed, whether or not a third party. Public authorities which may have access to personal data in the context of an individual investigation in accordance with Union or Member State law are not recipients; the processing of those data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing;
10. **"the data subject's consent" means a** freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject signifies, by a statement or by an act expressing his or her unambiguous consent, that he or she signifies his or her agreement to the processing of personal data concerning him or her;

11. **"personal data breach" means** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

12. **"pseudonymisation"** means the processing of personal data in such a way that it is no longer possible to identify the natural person to whom the personal data relate without further information, provided that such further information is kept separately and technical and organisational measures are taken to ensure that no association with identified or identifiable natural persons is possible;

13. **"filing system"** means a set of personal data, structured in any way, whether centralised, decentralised or structured according to functional or geographical criteria, which is accessible on the basis of specified criteria;

14. **"third party"** means a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct authority of the controller or processor, are authorised to process personal data;

15. **"genetic data"** means any personal data relating to the inherited or acquired genetic characteristics of a natural person which contains specific information about the physiology or state of health of that person and which results primarily from the analysis of a biological sample taken from that natural person;

16. **"biometric data"** means any personal data relating to the physical, physiological or behavioural characteristics of a natural person obtained by means of specific technical procedures which allow or confirm the unique identification of a natural person, such as facial image or dactyloscopic data;

17. **"health data"** means personal data relating to the physical or mental health of a natural person, including data relating to the provision of health services to a natural person which contains information about the health of the natural person;

18. **"enterprise"** means any natural or legal person carrying on an economic activity, regardless of its legal form, including partnerships or associations carrying on a regular economic activity;

19. **"group of undertakings"** means the controlling undertaking and the undertakings controlled by it;

20. **"Binding Corporate Rules"** means the rules on the protection of personal data followed by a controller or processor established in the territory of a Member State of the Union in one or more third countries in relation to the transfer or series of transfers of personal data by a controller or processor within the same group of undertakings or the same group of undertakings engaged in a joint economic activity;

21. **'supervisory authority'** means an independent public authority established by a Member State in accordance with Article 51;

22. **'relevant and reasoned objection'** means an objection to a draft decision, which concerns whether this Regulation has been infringed or whether the envisaged measure for the controller or processor is in compliance with this Regulation; the objection must clearly demonstrate the significance of the risks posed by the draft decision to the fundamental rights and freedoms of data subjects and, where applicable, to the free flow of personal data within the Union;

III. PRIVACY PRINCIPLES

1. LEGALITY, FAIR TRIAL, TRANSPARENCY

The processing of personal data must be lawful, fair and transparent for the data subject.

It should be transparent to natural persons how their personal data relating to them are collected, used, accessed or otherwise processed, and in what context the personal data are or will be processed.

Personal data must be adequate and relevant for the purposes for which they are processed.

Personal data must be processed in a manner that ensures an adequate level of security and confidentiality, inter alia, in order to prevent unauthorised access to or use of personal data and the means used to process personal data.

2. TARGET CONSTRAINTS

Personal data must be collected only for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes; Further processing for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes is not considered incompatible with the original purpose.

If the processing is for more than one purpose, consent must be given for all the purposes for which the data are processed.

If the data subject gives his or her consent following an electronic request, the request must be clear and concise and must not unnecessarily impede the use of the service for which consent is sought.

3. DATA SAVING

Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

Personal data may be processed only if the purpose of the processing cannot be achieved by any other reasonable means.

In order to ensure that the storage of personal data is limited to the necessary period, the controller will set time limits for erasure or periodic review.

Ensure that the storage of personal data is limited to the shortest possible period.

The data processed should be limited to the minimum necessary for the purpose.

4. ACCURACY

The personal data must be accurate, complete, current and, where necessary, up to date; all reasonable steps must be taken to ensure that personal data which are inaccurate for the purposes of the processing are erased or rectified without delay

5. LIMITED STORAGE

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data should be kept for longer periods only if the processing of personal data will be carried out for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures as provided for in this Regulation to safeguard the rights and freedoms of data subjects.

6. INTEGRITY AND CONFIDENTIALITY

Personal data must be processed in such a way as to ensure adequate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical or organisational measures.

7. OPENNESS ELVE

The fact, place and purpose of processing, the identity of the controller and the processing policy must be public.

8. ACCOUNTABILITY

The Controller is responsible for compliance with the Principles and must be able to demonstrate such compliance.

The controller shall take into account the state of science and technology and the costs of implementation, as well as the nature, scope, context and purposes of the processing and the varying degrees of risk to the rights and freedoms of natural persons, both in determining the means of processing, and in the course of the processing, it shall implement appropriate technical and organisational measures, such as pseudonymisation, aimed at ensuring the effective implementation of data protection principles, such as data minimisation, and at incorporating into the processing the necessary safeguards to meet the requirements of this Regulation and to protect the rights of data subjects.

The controller must implement appropriate technical and organisational measures to ensure that, by default, only personal data that are necessary for the specific purpose of the processing are processed.

IV. LEGAL BASIS FOR PROCESSING

1. VOLUNTARY CONSENT OF THE DATA SUBJECT

Pursuant to Article 6(1)(a) of the Regulation, processing may take place on the basis of the data subject's voluntary consent.

Where the Data Controller is not entitled to process the Data Subject's rights on the basis of any other legal basis, the Data Subject shall have the right to withdraw his or her consent to the processing, in whole or in part, or to request the erasure of his or her data, by written notice to the Data Controller.

In case of paper consent, the Data Controller is obliged to keep the consent form.

The controller must provide a pre-written consent form, which must be in an intelligible and easily accessible form, in clear and simple language and not contain unfair terms.

If the processing is for more than one purpose, consent must be given for all the purposes for which the data are processed.

In proceedings initiated at the request of the Data Subject, his or her consent to the processing of his or her necessary data and all the data he or she has provided shall be presumed. This fact shall be brought to the attention of the data subject. This includes the data provided by the Data Subject in the case of online, personal (paper) or telephone requests for quotations and room reservations.

In the case of children under the age of 16, the person who has parental authority over the child gives consent or authorises the processing.

The Controller shall make reasonable efforts, taking into account available technology, to verify that the consent has been given or authorised by the holder of parental responsibility over the child.

With regard to hotel guests, the Data Controller processes personal data concerning the physical or mental health of the Data Subject, including data concerning the Data Subject's food sensitivities, on the basis of the Data Subject's voluntary consent.

2. DATA REQUIRED FOR THE PERFORMANCE OF THE CONTRACT

Pursuant to Article 6(1)(b) of the Regulation, processing is necessary for the performance of a contract to which the Data Subject is a party or for taking steps at the request of the Data Subject prior to entering into the contract.

An important consideration in the design of the service is which data are necessary for the provision of the service, as they can also be processed on the basis of this legal basis. The contract

no further data may be processed in addition to the data necessary for the fulfilment of the request, solely on the basis of this legal basis.

With regard to hotel guests, unless additional data are necessary for the performance of the contract, the Data Controller processes the following data:

Data necessary to identify the Data Subject:

a) the name, place of residence and place of stay of the Data Subject;

b) the age and sex of the Data Subject;

c) the place and date of birth of the Data Subject;

d) the mother tongue of the Data Subject;

e) the email address of the Data Subject;

f) the telephone number(s) of the Data Subject;

g) the mobile phone number(s) of the Data Subject;

h) the bank details of the Data Subject (including: credit/debit card type, number, holder name, expiry date, CV code);

i) the registration number of the Affected Vehicle;
j) the identity card number of the Data Subject;

With regard to the hotel's partners, the Data Controller processes the following data, unless additional data are necessary for the performance of the contract:

a) the (business) name, residence, domicile or registered office, place of business or branch of the Data Subject;

b) the name of the representative of the Data Subject;

c) the name of the contact person of the Data Subject;

d) the email address of the Data Subject;

e) the telephone number(s) of the Data Subject;

f) the bank details of the Data Subject;

3. PROCESSING NECESSARY FOR COMPLIANCE WITH A LEGAL OBLIGATION OF THE CONTROLLER

The processing is necessary for the protection of the vital interests of the data subject or of another natural person pursuant to Article 6(1)(c) of the Regulation.

The Data Controller is entitled to use data processing that is legally binding on him or her (e.g. accounting standards).

4. PROCESSING FOR THE PROTECTION OF VITAL INTERESTS

Pursuant to Article 6(1)(d) of the Regulation, processing is necessary for compliance with a legal obligation to which the Controller is subject.

Such cases include processing for debt management purposes and where the data subject is a client of the Controller or employed by the Controller.

5. PROCESSING FOR THE PURPOSES OF LEGITIMATE INTERESTS

Pursuant to Article 6(1)(f) of the Regulation, processing is necessary for the purposes of the legitimate interests pursued by the Controller or a third party.

V. PROVISIONS ON DATA MANAGEMENT– INFORMATION ON DATA MANAGEMENT

1. THE SCOPE OF THE INFORMATION ON DATA PROCESSING

In the case of newly started processing, personal data relating to the data subject shall be collected by the Data Controller from the data subject at the time of obtaining the personal data, and, where the data subject subsequently requests information, the following information shall be provided to the data subject at the time of providing such information:

a) the identity and contact details of the Data Controller and, if appointed, of its representative;

b) contact details of the Data Protection Officer (the person responsible for data protection);

c) the purposes for which the personal data are intended to be processed and the legal basis for the processing (including, in particular, the legitimate interests of the Controller and third parties);

d) the recipients of the personal data, if any, the categories of recipients;

e) where applicable, the fact that the Data Controller intends to transfer the data to a third country or an international organisation, the existence or absence of a relevant adequacy decision or, in the case of such a transfer, an indication of the appropriate and suitable safeguards and a reference to the means of obtaining a copy or the availability of a copy;

f) the duration of the storage of personal data or, where this is not possible, the criteria for determining that duration;

g) informing the data subject of his or her right to request the Controller to access, rectify, erase or restrict (block) the processing of personal data relating to him or her and to object to the processing of such personal data, and of the data subject's right to data portability;

h) where the processing is based on the data subject's consent, information that he or she may withdraw his or her consent at any time, without prejudice to the lawfulness of the processing carried out on the basis of the consent before its withdrawal;

i) the data subject has the right to lodge a complaint with a supervisory authority;

j) whether the provision of the personal data is based on a legal or contractual obligation or is a precondition for the conclusion of a contract, whether the data subject is under an obligation to provide personal data and the possible consequences of not providing the data;

k) where relevant, the fact of automated decision-making, including profiling, and, at least in these cases, the logic used and the significance and likely consequences for the data subject of such processing.

If the Data Controller intends and has the possibility to process the personal data for a purpose other than the purpose for which they were collected, the Data Controller shall, subject to the applicable rules of the Regulation, inform the data subject of this other purpose and of all the information set out in the above points before the further processing.
In the case of newly started processing, where this is possible and where the personal data relating to the data subject are not collected by the Controller from the data subject, the Controller shall provide the data subject with the above information, the source of the personal data and, where applicable, whether the data originate from a publicly available source, at the time the personal data are obtained or when the information notice is drawn up.

VI. THE CONTROLLER RESPONSIBLE FOR DATA PROTECTION MATTERS

1. THE DATA PROTECTION OFFICER / CONTROLLER

Title: **Data Protection Officer / Data Controller**
Name: PINTAKOL KFT.
E-mail contact: thermalhotelgarden@gmail.com Telephone
contact: +36 20/ 215-8112

2. TASKS OF THE DATA PROTECTION OFFICER / CONTROLLER

The DPO shall inform the employer and provide professional advice to the employer and the employer's employees on their obligations under the General Data Protection Regulation and other EU and Hungarian data protection provisions and:

- monitor compliance with the General Data Protection Regulation and other EU and Hungarian data protection provisions, as well as the employer's internal rules on the protection of personal data, including the assignment of responsibilities, awareness raising and training of staff involved in data processing operations, and related audits;

- the employer shall, upon request, provide technical advice on the data protection impact assessment and monitor the performance of the impact assessment; investigate the notifications received and, if unauthorised processing is detected, request the controller or processor to cease the processing;

- keeps internal data protection records;

- ensure data protection education

- cooperate with the supervisory authority responsible for data protection matters;

- acts as a contact point for the supervisory authority on all matters relating to the employer's data management and consults the supervisory authority on any other matter.

In addition to the above, the Data Protection Officer is entitled to:

- propose the establishment of a data protection guarantee scheme,
- propose the content of data protection policies,

- conduct a data protection audit,

- contributes to the selection of data processors,

- contributes to the negotiation of data processing contracts,

- contribute to the control of data processors.

The Data Protection Officer shall assist the work of the departments carrying out data processing and data handling with his/her advice and opinions, and shall monitor the lawfulness of data processing and data handling at the Data Controller. He shall carry out audits of individual processing operations as necessary. The Data Protection Officer shall inform the Executive Director in writing of the findings of the audit.

The Data Protection Officer shall have the right to access the processing and the related records of all departments of the Data Controller. He may ask the head of the unit and his staff for information, either orally or in writing. You may consult

the DPO is bound by confidentiality obligations in relation to personal data obtained during the investigation.

If a breach of the law is detected, the DPO will assist in restoring the lawfulness of the processing or, if this is not feasible, may require the controller to cease processing.

3. THE RIGHTS OF THE DATA PROTECTION OFFICER / CONTROLLER

To fulfil the duties of the internal data protection officer:

- any procedural or organisational measures relating to data management, or changes thereto, may only be introduced after approval by the internal data protection officer;

- all departments and persons must provide the information requested within the prescribed time limit;

- all managers are required to examine the substance of any comments they make on data management and to give their opinion on request within the prescribed time limits;

- the head of the area concerned is responsible for implementing the proposal he/she has made to ensure compliance with the provisions on data protection, once it has been accepted by the organisation responsible for its professional management, and for keeping the internal data protection officer informed;

- it is the responsibility of all managers in the area of personal data processing to inform the DPO of their proposals on how to keep personal data in a structured file and how to make them aware of the data management principles laid down in the applicable legislation;
- the internal data protection officer must be notified of all projects that affect his or her activities;

- all employees of the Data Controller are obliged to inform the internal Data Protection Officer of any unlawful processing or processing activity

  (see III. Data Protection Principles).

VII. THE RIGHTS OF THE DATA SUBJECT

The Data Subject has the following rights in the event of processing by the Data Controller:

1. INFORMATION AND ACCESS TO PERSONAL DATA

The Data Subject has the right to access his or her personal data held by the Data Controller and information about their processing, to request at any time, to check what data the Data Controller holds about him or her, and to have access to the personal data. The Data Subject shall provide the Controller with his or her request for access to the data in writing and shall provide the requested data in writing

(electronically or by post), the Data Controller will not provide any oral information in this context. The data subject shall have the right to request at any time information about the personal data concerning him or her processed by the Controller.

In case of exercise of the right of access, the information shall include the following data:

- define the scope of the data processed,

- the purpose, time and legal basis of the processing in relation to the scope of the data processed,

- transfer: to whom the data have been or will be transferred,

- Indicate the data source.

the Data Controller provides the data subject with a paper or electronic copy of the personal data free of charge for the first time. For additional copies requested by the data subject, the Controller may charge a reasonable fee based on administrative costs. Where the data subject requests a copy by electronic means, the Controller shall provide the information to the data subject by e-mail in a commonly used electronic format.

If the data subject does not agree with the processing and the accuracy of the data processed, he or she may request the rectification, supplementation, erasure or restriction of the processing of personal data concerning him or her, or object to the processing of such personal data, in accordance with the provisions of this Policy.

The Data Controller shall provide the requested information within 30 days upon request.
In the context of the information, the person responsible for data protection - or the data processor designated for this task in the contract - shall provide information on the data concerning the data subject processed by the Data Controller and on the above.

The information shall be provided in the form requested by the data subject, in the absence of an explicit request, primarily by email and secondarily by post, provided that the Data Controller has the necessary data for the use of the form of communication and that the identity of the data subject can be established beyond doubt.

If the Data Controller can demonstrate that it is not in a position to identify the data subject, it shall, where possible, inform the data subject accordingly by appropriate means. In such cases, the data subject's right of access, right to rectification and erasure, right to restriction of processing, right to notification and right to data portability shall not be granted by the Controller unless the data subject provides additional information allowing his or her identification in order to exercise his or her rights under those provisions.

Employees and other persons involved in the processing of personal data are obliged to provide information on the handling of complaints to the person responsible for data protection.

Before disclosing information that is considered a trade secret or bank secret over the phone, the caller must provide at least two identifiable pieces of information about the customer: his or her mother's name and place or date of birth.

2. THE RIGHT TO RECTIFY OR SUPPLEMENT THE DATA PROCESSED

At the request of the data subject, the Data Controller shall, without undue delay, correct inaccurate personal data provided by the data subject in writing or complete incomplete data with the content indicated by the data subject. The Data Controller shall inform any recipient to whom the personal data have been disclosed of the rectification or completion, unless this proves impossible or involves a disproportionate effort. The data subject shall be informed of the data of such recipients if he or she so requests in writing.

3. THE RIGHT TO RESTRICT PROCESSING

The data subject shall have the right to obtain, upon written request, restriction of processing by the Controller if.

- the data subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the Controller to verify the accuracy of the personal data,

- the data processing is unlawful and the data subject opposes the erasure of the data and requests instead the restriction of their use,

- the Controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims,

- the data subject objects to the processing; in this case, the restriction shall apply for the period until it is established whether the legitimate grounds of the Controller prevail over the legitimate grounds of the data subject.

The Data Controller shall inform the data subject at whose request the processing has been restricted in advance of the lifting of the restriction.

4. THE RIGHT TO ERASURE (FORGETTING)

At the request of the data subject, the Data Controller shall delete personal data concerning the data subject without undue delay where one of the grounds specified applies:

i) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed by the Controller;

ii) the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;

iii) the data subject objects to the processing for reasons relating to his or her particular situation and there are no legitimate grounds for the processing;

iv) the data subject objects to the processing of personal data relating to him or her for direct marketing purposes, including profiling, where it is related to direct marketing;

v) the personal data are unlawfully processed by the Controller;

vi) personal data are collected in connection with the provision of information society services directly to children.

The data subject may not exercise his or her right to erasure or blocking if the processing is necessary

i) to exercise the right to freedom of expression and information;

ii) in the public interest in the field of public health;

iii) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, where the exercise of the right of erasure would make such processing impossible or seriously impair it; or

iv) to bring, enforce or defend legal claims.

5. RIGHT TO DATA PORTABILITY

Data portability allows the data subject to obtain and further use the "own" data that he or she has provided to the Data Controller's system, for his or her own purposes and through different service providers. In all cases, the right is limited to the data provided by the data subject, and there is no portability of other data (e.g. statistics, transaction data, etc.)

The data subject shall provide the personal data relating to him or her that are held by the Controller:

- in a structured, widely used, machine-readable format,
- to another controller,
- may request the direct transfer of the data to another controller - if technically feasible in the controller's system.

The Data Controller shall only comply with a request for data portability on the basis of a request sent by e-mail or post. In order to comply with the request, the Data Controller must ensure that the data subject who is entitled to exercise the right intends to do so. This requires the data subject to provide the Controller, in his request, with the data which he has provided to the Controller on the Website or otherwise, in order to enable the Controller to identify the data subject making the request using the data contained in its system. The data subject may, in the context of this right, request the portability of data at most of those which he or she has voluntarily

provided to the Data Controller. The exercise of this right does not automatically entail the deletion of the data from the Controller's systems.

6. OBJECTION TO THE PROCESSING OF PERSONAL DATA

The data subject may at any time object to the processing of his or her personal data, including profiling, on grounds relating to his or her particular situation, and the data subject shall have the right to object at any time to the processing of personal data concerning him or her for direct marketing purposes, including profiling. If the data subject objects to the processing of personal data for direct marketing purposes, the personal data shall no longer be processed by the Controller for those purposes.

The Controller may no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The data subject may object in writing (by e-mail or by post).

VIII. INTERNAL PROCEDURES FOR THE EXERCISE OF THE RIGHTS OF THE DATA SUBJECT

The Data Controller shall inform the data subject of the measures taken without undue delay and in any event within one month of receipt of any request. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months, but in that case the Data Controller shall inform the data subject within one month of receipt of the request, stating the reasons for the delay. Where the data subject has made the request by electronic means, the information shall be provided by the Controller by electronic means, unless the data subject requests otherwise. If the Controller does not comply with the data subject's request for any reason, it shall give reasons for not doing so.

If the data subject does not exercise his or her rights in person, the person responsible for the procedure must have a power of attorney in the form of a private document with full probative value, which must be attached to the documents submitted to the Data Controller.

1. HANDLING A REQUEST FOR DELETION

The data subject shall have the right to obtain from the Data Controller the erasure of personal data relating to him or her without undue delay and the Data Controller shall be obliged to erase personal data relating to him or her without undue delay if one of the following grounds applies:

a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

b) the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;

c) the data subject objects to processing necessary for the public interest or for the purposes of the legitimate interests pursued by the Controller or a third party and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of data obtained for direct marketing purposes;

d) the personal data were unlawfully processed by the Controller;

e) the personal data must be erased in order to comply with a legal obligation under Union or Member State law applicable to the Data Controller;

f) personal data are collected in connection with the provision of information society services under the Regulation.

Where the Data Controller has disclosed the personal data and is obliged to delete it, it shall take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform the Data Controllers that process the data that the data subject has requested the deletion of the links to or copies or replicas of the personal data in question.

The erasure need not be carried out if the processing is

a) necessary for the exercise of freedom of expression or the right to information,
b) necessary for the establishment, exercise or defence of legal claims,

c) necessary in the public interest in the field of public health,

d) necessary to comply with a legal obligation,

e) is necessary for archiving purposes in the public interest, scientific or historical research, statistical purposes and the deletion of the data would make it impossible or seriously jeopardise the purpose of the processing.

The controller shall also erase or anonymise personal data relating to the data subject contained in its computerised systems and paper records, unless otherwise provided by law and the purpose for which the personal data are processed has ceased to exist. Where the erasure of personal data cannot be achieved without prejudice to the document containing the personal data:

a) where the Data Controller or a third party has a legitimate interest in the retention of the document, the Data Controller shall keep the document for the period specified in the rules on records management, shall keep the document in closed form in the event of a request for its deletion and shall inform the data subject thereof, and shall destroy the document together with the personal data after the expiry of the period specified in the rules on records management,

b) if neither the Data Controller nor any third party has a legitimate interest in keeping the document, destroy the document together with the personal data.

In all cases, the person responsible for data protection shall take measures for the deletion of the data in cooperation with the department or IT system administrator concerned with the processing of personal data.

The Data Controller shall delete the personal data irretrievably from its IT systems, where possible, and shall ensure that the deletion of the personal data is also reflected in the archived version of the IT system. The person responsible for the IT system shall be responsible for the deletion.

If irreversible deletion is not feasible for IT reasons, the Data Controller shall carry out logical deletion of the data. In the context of logical erasure, the personal data shall be replaced by an identifier that prevents further data relating to the personal data from being subsequently associated with the data subject.

In the case of paper documents, their destruction must be recorded.

The report shall record: the type of documents destroyed, the information necessary for the identification of the documents destroyed, the date of destruction and the name and position of the person who carried out the destruction, and, in the case of an external partner, the name of the external partner.

If the deletion of the data is required by law, but is not possible for legitimate interests of the data subject, the personal data or the electronic or paper documentation containing the personal data shall be blocked. In this case, only the administrator of the IT system or the person responsible for data protection shall have access to the data or documents stored in the IT system. In the case of paper documentation, the document shall be kept in a lockable cabinet.

The Data Controller shall terminate users' access to electronic copies of paper documents uploaded to the internal system.

2. HANDLING OF OBJECTIONS TO DATA PROCESSING

The data subject must be given the right to object to the processing of his or her personal data. The person responsible for data protection shall identify the data subject as soon as possible, examine the objection within the shortest possible time from the date of the request, decide whether the objection is justified and inform the applicant of his or her decision.

The Data Controller's internal data protection officer shall examine the objection, with the simultaneous suspension of processing, within a maximum of 15 days from the date of the request and inform the Data Subject in writing of the outcome.

If the objection is justified, the Data Controller is obliged to terminate the processing, including further data collection and transmission, and to block the data, and to notify the objection and the measures taken on the basis of the objection to all those to whom the personal data concerned by the objection were previously transmitted and who are obliged to take action to enforce the right to object.

3. HANDLING A CORRECTION REQUEST

The data subject has the right to request the rectification of incorrectly recorded data at any time. The data subject shall have the right to request that incomplete personal data be completed, including by means of a supplementary declaration.

If the data subject indicates that any of the data processed by the Data Controller is inaccurate, the person responsible for data protection shall identify the data subject and ensure that the data is corrected, and shall, as part of his or her procedure, notify the administrator of the relevant IT system of the Data Controller of the request for correction of the data, indicating the correct data.

If the correct data is not available, the person responsible for data protection will ask the data subject for clarification of the correct data.

If the correct data cannot be established, the person responsible for data protection shall ensure that the incorrect data is blocked. Blocking means putting the data in a passive state and informing the data subject that the data cannot be rectified in the absence of correct data, but that the data have been blocked.

The Controller shall correct the incorrect data within 48 hours.

4. PROCESSING A REQUEST FOR RESTRICTION OF PERSONAL DATA

The data subject shall have the right to obtain from the Data Controller, at his or her request, the restriction of processing if one of the following conditions is met:

- the data subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the Controller to verify the accuracy of the personal data;

- the processing is unlawful and the Data Controller opposes the erasure of the data and requests instead that the data be
  restrictions on the use of;

- the controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims; or

- the data subject has objected to the processing, but the legitimate interests of the Controller may also justify the processing, in which case the processing must be restricted until it is established whether the legitimate grounds of the Controller prevail over the legitimate grounds of the data subject.

If the processing is restricted, such personal data may be processed, except for storage, only with the consent of the data subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or of an important public interest of the Union or of a Member State.

The controller shall inform the data subject at whose request the processing has been restricted of the lifting of the restriction in advance.

IX. ENFORCEMENT OPTIONS

You can exercise your rights by sending a request by e-mail or by post. No rights can be exercised by telephone.

The data subject can exercise his or her rights by contacting:

Name: PINTAKOL KFT.
Address for correspondence: 4200 Hajdúszoboszló Debreceni út
6. Phone number: +36 20 / 215-8112
E-mail address: thermalhotelgarden@gmail.com

The data subject cannot enforce his or her rights if the Controller proves that he or she is not in a position to identify the data subject. Where the data subject's request is manifestly unfounded or excessive (in particular in view of its repetitive nature), the Controller may charge a reasonable fee for complying with the request or refuse to act. The burden of proof shall lie with the Controller. If the Controller has doubts about the identity of the natural person who has made the request, it may request further information necessary to confirm the identity of the applicant.

The data subject is entitled, pursuant to the Regulation and the Civil Code (Act V of 2013)

- You can contact the National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/c.; www.naih.hu) or

- You can enforce your rights in court.

X. DATA BREACH MANAGEMENT

1. THE CONCEPT OF DATA BREACHES

A data breach is a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. The Data Controller shall keep a register for the purposes of monitoring the measures taken in relation to the personal data breach, informing the supervisory authority and informing the data subject, which shall include the scope of the personal data affected by the breach, the number and type of data subjects, the date of the breach, the circumstances of the breach, its effects and the measures taken to remedy the breach. Where the Controller considers that an incident presents a high risk to the rights and freedoms of data subjects, it shall inform the data subject and the supervisory authority of the personal data breach without undue delay and within a maximum of 72 hours.

A personal data breach may, in the absence of adequate and timely action, cause physical, material or non-material damage to natural persons, including to their personal data

loss of control or restriction of their rights, discrimination, identity theft or misuse, financial loss, unauthorised use of pseudonymisation, damage to reputation, damage to the confidentiality of personal data protected by professional secrecy or other significant economic or social disadvantages suffered by the natural persons concerned.

2. REPORTING DATA BREACHES

Persons subject to this Policy shall, in the case of any IT system operated by or with the assistance of the Data Controller, report to the Data Protection Officer without undue delay, but no later than 12 hours, if they suspect a data breach or if they are aware that a data breach has occurred.

The notification must be made primarily during working hours, by telephone, and must also be confirmed by electronic mail at the request of the Data Protection Officer.

3. THE PROCEDURE TO BE FOLLOWED IN THE EVENT OF A DATA BREACH

The person responsible for data protection and other persons concerned shall act in accordance with the provisions of this Chapter in order to detect and determine the seriousness of a personal data breach reported to them or established within their competence.

The Data Controller will take all necessary measures to avoid any data breaches. If a data breach does occur:

a) The person responsible for data protection shall contact the administrator of the IT system involved in the data breach, the data controller of the data processing operation involved in the data breach and, if identifiable, the person who caused the incident.

b) The person responsible for data protection must classify the personal data breach in one of the following categories:

- Low-level personal data breach: unauthorised disclosure, alteration, disclosure, intentional or unintentional deletion or destruction of a negligible amount of personal data or other unlawful processing.

- A medium level personal data breach: the alteration, unauthorised disclosure, unauthorised transmission, disclosure, intentional or unintentional deletion or destruction of a small amount of personal data or other unlawful processing.

- High level data breach:

  - unauthorised alteration, disclosure, disclosure, intentional or unintentional deletion or destruction of a wide range of personal data or any other unlawful processing; or

- irrespective of the scope of the data, any case where the incident is likely to have an adverse effect on the data subject or is certain to have an adverse effect on the data subject.

c) In the event of a low-level personal data breach, the person responsible for data protection:

- determine with the system administrator of the system concerned and the data controller of the data processing operation affected by the personal data breach how the personal data breach will be handled and notify the person authorised to take action of the personal data breach
  Treatment,

- record the data protection incident in the incident log.

d) In case of a medium level data breach:

- the person responsible for data protection convenes a working group without delay, but no later than 12 hours after becoming aware of the data breach, in which, in addition to the person responsible for data protection, the administrator, the data controller of the data processing operation affected by the data breach and the head of the Data Controller participate,

- the Working Party determines how to deal with the incident and refers the incident to the person authorised to take action,

- the person responsible for data protection records the data protection incident in the incident register,

- the person responsible for data protection notifies the supervisory authority of the personal data breach within 72 hours if the personal data breach is likely to result in a risk to the rights and freedoms of the data subject or other data subjects.

e) In case of a high-level data breach

- the person responsible for data protection convenes a working group immediately, but no later than 12 hours after becoming aware of the incident, with the participation of the administrator, the person responsible for data protection, the person responsible for the incident
  the data controller of the data processing operation concerned and the head of the controller,

- the Working Party shall determine how the personal data breach shall be handled and shall call upon the person authorised to act to handle the personal data breach and, where necessary, determine how the data subjects shall be notified and the content of the notification; and
  ensure that the persons concerned are notified without delay.

- the person responsible for data protection records the data protection incident in the incident register,

- the person responsible for data protection notifies the supervisory authority of the data breach within 72 hours of becoming aware of it.

The Data Controller shall, through the Data Protection Officer, keep a record of the personal data breaches for the purpose of monitoring the measures taken in relation to the personal data breach and informing the data subject, including the scope of the personal data affected by the personal data breach, the number and scope of the data subjects affected by the personal data breach, the date, circumstances, effects and measures taken to remedy the personal data breach, and other data specified in the legislation providing for data processing.

4. INFORMATION ON DATA BREACHES

If so requested by the data subject, the data protection officer will provide information on data breaches involving the data subject's personal data.

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the personal data breach in writing or, if an email address is available, by email without undue delay.

The notification must clearly and plainly describe the nature of the data breach and include at least the following information:

- the name and contact details of the person responsible for data protection or other contact person who can provide further information;

- explain the likely consequences of the data breach;

- describe the measures taken or envisaged by the Data Controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

The controller is not obliged to inform the data subject of the personal data breach if.

- The data controller has implemented appropriate technical and organisational protection measures and applied these measures to the data affected by the personal data breach (in particular, measures such as the use of encryption to make the data unintelligible to persons not authorised to access the personal data).

- The controller has taken additional measures following the personal data breach to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

- The provision of information would require a disproportionate effort on the part of the Data Controller. In such cases, the data subjects shall be informed by means of publicly disclosed information or by a similar measure which ensures that the data subjects are informed in an equally effective manner. For example, issuing a press release.

If the Data Controller has not notified the data subject of the personal data breach, the supervisory authority may, after having considered whether the personal data breach is likely to result in a high risk, order the data subject to be informed or determine that the data subject does not need to be informed for one of the reasons set out in the previous point.

A data protection incident may occur not only at the Data Controller, but also at the data processor under contract with the Data Controller. If the data processor detects a data breach in its system, it shall notify the Data Controller without undue delay or, if it is not possible to communicate the information at the same time, it shall communicate it in full or in part without undue delay.

Liability for failure to notify a data breach lies with the data processor who fails to notify.

If the Data Controller becomes aware of a data breach at one of its Processors, or if a data breach is suspected, the Data Controller shall, by simultaneously notifying the Processor, carry out the procedure for identifying and handling the data breach in accordance with this point.

XI. ADATABILITY

The Data Controller undertakes to ensure the security of the data, to take technical measures to ensure that the data recorded, stored or processed are protected and to take all necessary measures to prevent their destruction, unauthorised use or unauthorised alteration. It also undertakes to require any third party to whom it may transfer or disclose the data to comply with its obligations in this respect.

The Data Controller shall ensure, by appropriate technical means, that data stored in different registers cannot be directly linked and attributed to the data subject, except where permitted by law, in order to protect the electronically processed data files.

The employees of the Data Controller's departments carrying out data processing or processing are obliged to keep the personal data they have access to as bank or business ticks.

1. DATA STORED ON A COMPUTER

In particular, the following measures must be taken to ensure the security of personal data stored on computers and networks:

- The data and databases must be stored in a room with fire and property protection equipment.

- Access to data is only possible with valid, personal, identifiable access rights - at least a user name and password. Network resources can only be accessed with a valid user name and password. To change passwords
  must be regularly looked after.

- The passive part of the databases containing personal data - the data that do not need further processing and remain unchanged - should be separated from the active part and the passivated data should be recorded on a durable medium. For the purposes of this Code
  the archiving of the data processing referred to in the specific part of this Article shall be carried out once a year. The data medium containing the archived data shall be kept in a fireproof metal box or cabinet.

- All workstations of the Data Controller, and in particular the computers of administrators processing personal data, shall be provided with real-time virus protection.
- Unauthorised persons must be prevented from gaining access to servers storing data that are accessible via the network, using the computer tools available at all times.

- The network server (hereinafter referred to as "**server**") must be secured by continuous mirroring on a physically separate storage medium to avoid the loss of personal data.

- Active data in databases containing personal data should be regularly backed up on a separate medium. The backup medium shall be kept in a fireproof metal box/cabinet.

2. MANUALLY MANAGED DATA

To ensure the security of personal data processed manually, the following measures must be taken for all areas affected by data security:

- Documents held in the archives must be kept in a lockable, dry room with fire and property protection equipment.

- Only the competent administrators have access to documents that are under active management or archived on a permanent basis.

- The archiving of records of data processing should be carried out once a year. The archived documents shall be sorted and archived in accordance with the Data Controller's filing policy and filing plans.

XII. <u>DATA SUPPLY</u>

Where personal data is also bank or trade secret data, the processing must comply with all applicable legal provisions.

The personal data processed must comply with the following requirements:

- their recording and handling is fair and lawful;
- are accurate, complete and, where necessary, timely;
- the way in which they are stored is such that the Data Subject can be identified only for the time necessary for the purpose for which they are stored.

XIII. DATA TRANSMISSION

1. GENERAL PROVISIONS

Personal data may only be transferred and different processing operations may only be combined if the Data Subject has given his or her written consent or if permitted by law and if the conditions for processing are met for each individual personal data.

All data processing disciplines that are involved in the transfer of personal data must keep a transfer register.

The duration of the registration - and, on this basis, the obligation to provide information - may be limited by the law governing the processing. The period of restriction may not be less than five years in the case of personal data.

For lawful operation, both the purpose and duration (expiry date) of the data transfer or interconnection must be taken into account.

2. DATA TRANSMISSION BASED ON A SENDING REQUEST

A request for disclosure of data from an organisation or individual other than the Data Controller may only be fulfilled if the Data Subject authorises the Data Controller to do so in writing. The Data Subject may also give such an authorisation in advance, which may be for a specified period and to a specified number of bodies to which the request is addressed. The fact of the transfer shall be recorded in writing and the DPO shall be informed of the fact of the transfer.

Regardless of the declaration of the Data Subject, in the cases provided for by the applicable legislation, requests received from the competent authorities, public bodies, offices, in particular: police, courts, prosecutor's office, NAV, social security, as well as from the national security services, notary in probate proceedings, etc. Such requests shall be treated according to the classification given by the data requester and the Data Subject shall not be informed of the fact of the request. Requests from these bodies shall be communicated to the internal Data Protection Officer by the competent department. The provisions of other legislation on personal data (e.g. Civil Code) shall also apply to the transfer of data relating to requests.

A transfer of personal data to a third country or to an international organisation may take place if the Data Subject has given his or her explicit consent or if the European Commission has determined that the third country, a territory or one or more specific sectors of the third country or the international organisation in question

organisation provides an appropriate level of protection. Such transfers do not require a specific authorisation.

XIV. GENERAL PROVISIONS FOR DATA PROCESSORS

The Data Controller and the data processors it employs are responsible for the processing, modification, deletion, transmission and disclosure of personal data. The processor shall not take any substantive decision regarding the processing, shall process personal data of which it becomes aware only in accordance with the provisions of the Controller and the contractual relationship between the Controller and the Clients, and shall not process such data for its own purposes, and shall store and retain the personal data in accordance with the provisions of the Controller.
The contract for the processing of data must be in writing. The creation of a data processing chain is prohibited, i.e. a processor may not further outsource data processing activities.

It must be included in the data processing contract:

-the duration of processing, o

- after the expiry of the deadline for returning the data, -

- or processing side.

A data processing contract may only be concluded with a processor established in an EEA Member State or in a country with the same level of data protection as the Regulation. Data transfers may also only be made from/to such countries. Transfers of personal data to a third country or an international organisation may take place if the Commission has determined that the third country, a territory or one or more specific sectors of the third country or the international organisation in question provide an adequate level of protection. Such transfers do not require a specific authorisation.

Where the legal relationship between the Data Controller and the data subject is for the purpose of processing, the data may be transferred without the consent of the natural person concerned (Data Subject), but after the Data Controller has been informed of the fact that the data processor has been used, and subject to the responsibility of the Data Controller. In such a case, the Data Controller's Chief Executive shall authorise the service provider to process the data in writing.

A specific list of the Company's data processors may be requested by writing to thermalhotelgarden@gmail.com, and the Data Controller will respond to such requests in writing within thirty (30) days.

XV. PROCESSING FOR COMMERCIAL PURPOSES

Eger-Park Hotel Ltd. processes the personal data of the Data Subjects in order to facilitate business transactions by providing its services and offers to the recipients under the conditions set out below.

1. THE SCOPE OF PERSONAL DATA PROCESSED BY THE CONTROLLER, THE PURPOSES OF THE PROCESSING AND THE LEGAL BASIS FOR THE PROCESSING

Data necessary to identify the Data Subject:

g) the name, place of residence and place of stay of the Data Subject;

h) the age and sex of the Data Subject;

i) the email address of the Data Subject;

j) the telephone number(s) of the Data

Subject; the purpose of the processing of the

listed data:

a) the identification of the Data Subject

b) to communicate with the Data Subject;

c) Recommend the services of the data controller.

The legal basis for processing is the consent of the data subject.

Data processed with the data subject's consent for the purposes of automated individual

decision-making: the data listed above.

A listed on data processing purpose: the Data subject listed on of the listed data of the Data Subject's Listed Data solely by means of a computer tool.

2. THE DURATION OF THE STORAGE OF PERSONAL DATA

From Data Controller on Data Subject consent revocation of consent stored by to the 1. the data specified in point.

3. HOW THE PERSONAL DATA IS STORED

The data processed by the Data Controller is stored in the following manner:

The Data Controller shall store the data specified in point 1 in the following ways, according to the way in which they are generated:

a) store the data that it processes on the basis of a written declaration in the original written

form or in the form of an electronic copy of the original document for the duration of the processing as defined in point 2;

b) store in electronic form data generated on the basis of declarations not made in writing or on the basis of consent given electronically.

4. THE CASES OF TRANSFER OF PERSONAL DATA

The data listed in point 1 are those who carry out processing activities on behalf of the Data Controller on behalf of the Data Controller.

The sub-processors shall be bound by the same confidentiality obligations as the Data Controller in relation to the data transferred as described above.

The data listed in point 1 may, with the consent of the Data Subject, be disclosed to third parties for commercial purposes, subject to the same confidentiality obligations as the Data Controller.

5. CARRYING OUT BUSINESS ACQUISITION ACTIVITIES

In the course of its business activities, the Data Controller guarantees to the Data Subject the enforcement of the rights set out in the Regulation, the Info Act and Act CXIX of 1995 on the processing of name and address data for research and direct marketing purposes (hereinafter: the Direct Marketing Act); and ensures that the requirements set out in the Regulation, the Info Act and the Direct Marketing Act are met in relation to the Data Controller's activities in the processing of the Data Subjects' personal data, in particular the obligation to ensure the secure processing of data.

The Data Controller shall provide the Data Subject with the possibility to withdraw his or her consent at any time in person at the Data Controller's registered office, by letter or by electronic mail.

6. NEWSLETTER AND DIRECT MARKETING

Technologically, the sending of newsletters (direct marketing) includes messages sent by electronic mail or equivalent means of individual communication (e-mail, SMS, mms, and fax), the content of which falls within the following definitions:

- business advertising (any communication, information or representation intended to promote the sale or otherwise obtain the use of movable tangible property, including money, securities and financial assets and natural resources which can be used as property, services, immovable property or rights in rem, or, in connection with such purpose, to promote the name, designation or activities of an undertaking or to increase the recognition of goods or trademarks),

- information related to the achievement of a social objective, which does not constitute advertising, and,

- communications the sole purpose of which is to request consent to the sending of an electronic advertisement,

- under the E-Commerce Act, electronic advertising is any information society service or advertisement communicated by means of electronic communications, with the exception of voice telephony, and information related to the achievement of a social objective which does not constitute advertising.

Advertising (advertisement) may only be communicated by directly contacting the Data Subject as the recipient of the advertisement (DM = Direct Marketing), in particular by e-mail or other equivalent means of individual communication (e.g. SMS), if the recipient of the advertisement (the Data Subject) has given his/her prior, clear and explicit consent (consent).

The Data Controller operates a newsletter sending function based on its direct marketing activities. The newsletter sending function is operated by the Data Controller with the assistance of a data processor.

The Data Controller shall provide the Data Subject with the possibility to withdraw his or her consent at any time in person at the Data Controller's registered office, by letter or by electronic mail.

In the case of online newsletters, it is not possible to tick the checkbox to give consent in advance.

With regard to consent to data processing for direct marketing purposes, the Data Subject may give his or her consent separately from the consent to data processing. A separate check-box is required for the data subject's consent to processing for direct marketing purposes. The privacy notice is placed next to the check-box and can be accessed by clicking on the link. In the case of direct marketing, it is not possible to tick the checkbox to give consent in advance.

Consent to data processing for direct marketing purposes includes

- the name of the contributor

- and the personal data that you wish to consent to the processing of (for example, your e-mail address or telephone number to which you wish to receive advertisements).

If the content of the advertisement to be sent is of an age that should only be sent to persons over a certain age, the consent will include the place and date of birth of the Data Subject.

The Data Processor shall keep an up-to-date record of the prior consents given and shall ensure that the Data Subject has the right to withdraw consent at any time, without giving reasons and free of charge.
You may also consent to the sending of advertising material by providing your address.

The Data Controller will review the newsletter list every five years and will ask for confirmation of consent to send the newsletter after five years. The data of a data subject who does not give his or her consent to the sending of the newsletter shall be deleted by the Controller within 30 days of the delivery of the e-mail.

To subscribe to the news feed posted on the Facebook wall on the Guest on page "like"/ "like" link by clicking to subscribe up, and at from the same website at
"You can unsubscribe by clicking on the "dislike" link or delete unwanted feeds from the message wall using the message wall settings.

XVI. WEBSITE OPERATION AND "COOKIES" - K

The legal basis for data processing in connection with the operation of the Website is the voluntary consent of the data subject. Communication through websites is a common way of reaching and informing customers and clients.

1. "COOKIE"- K

The Data Controller and the designated external service providers place and read back a small data package, a so-called cookie, on the computer of the data subject in order to provide a personalised service. If the browser returns a previously saved cookie, the cookie management service provider has the possibility to link the data saved during the data subject's current visits with the data saved during previous visits, but only with regard to its own content.

The Data Controller uses the following cookie:

- Session cookie: session cookies are automatically deleted after the data subject's visit. These cookies are used to make the Controller's Website more efficient and secure, i.e.
  are necessary for certain features of the Website or certain applications to function properly.

- Persistent cookies: persistent cookies are also used by the Data Controller to improve the user experience (e.g. to provide optimised navigation). These cookies are stored for a longer period of time in the browser's cookie file. The duration of the cookie is limited to the duration of the cookie.
  depends on the setting of the internet browser used by the data subject.

- Security cookie.

The "Help" function in the menu bar of (most) browsers provides information on whether the data subject can, in his or her own browser.

- how to disable cookies,
- how to accept new cookies,
- how to instruct your browser to set a new cookie, or - how to turn off other cookies.

➢ Cookies set by Google Analytics (cookies)

Google Analytics is an analytics service provided by Google Inc. ("Google"). Google Analytics uses cookies stored on users' computers to analyse their interactions with the

Website. The legal basis for the processing of data for web analytics purposes is the Website

the voluntary consent of the user. Cookies for analytical purposes (cookies) are anonymised and aggregated data that make it difficult to identify the computer, but cannot be excluded.

The analytical information collected by Google Analytics cookies is transmitted to and stored by Google on its servers. This information is processed by Google on behalf of the operator of the website in order to evaluate users' browsing habits, compile reports on the frequency of use of the website and provide other services related to the use of the website to the website operator.

More information about the cookies used by Google can be found at the following link: http://www.google.com/policies/technologies/ads/

A Google Privacy statement available at at the following link: http://www.google.com/intl/hu/policies/privacy/.

- Cookies set by Facebook (cookies)

The Data Controller operates a Facebook page, which is directly accessible from its website.

Facebook will also place cookies on your computer and you can find out more about them at https://hu-hu.facebook.com/policies/cookies/, where you can also find out how to block cookies.

The Website may also contain links to external servers (not managed by the data controller or processors) and the sites accessible through these links may place their own cookies or other files on your computer, collect data or request personal data. The controller disclaims any liability for these.

The Data Controller may use the data collected by the Cookies to send targeted advertising messages. The cookie is used to track the user across multiple websites. The Data Controller shall provide the Data Subject with the possibility to withdraw his/her consent at any time, either in person at the Data Controller's headquarters or by electronic mail.

2. REGISTRATION AT THE INITIATIVE OF THE DATA SUBJECT ON A WEBSITE, COMMUNITY OR ON A FORM

The legal basis for processing is the voluntary consent of the Data Subject in connection with registration.

The Data Subject may participate in the registration if the Data Subject accepts the terms of the Privacy Policy prior to registration via chekbox. The privacy notice is placed next to the chek-box and can be accessed by clicking on the link. The checkbox cannot be ticked in advance.

The Processor shall ensure that the Data Subject has the right to withdraw consent at any time, without giving any reason and free of charge.

Data processing time: in the event of cancellation of registration, the Data Controller will delete the data within 15 days of cancellation.

3. WEBSITE VISIT DATA

The Data Processor's website may also contain links that are not operated by the Company and are provided for the sole purpose of providing information to visitors. The Data Processor has no control over the content and security of websites operated by partner companies and is therefore not responsible for them.

4. FACEBOOK PAGE

The hotel operated by the Data Controller is available on the Facebook community portal.

The purpose of the processing is the sharing of exclusive content on the websites of the Data Controller, as well as content not found on those websites. The Facebook page allows guests to book rooms, participate in competitions and find out about the latest promotions.

By clicking on the "like" link on the Facebook page of the Data Controller, the Data Subject consents to the publication of news and offers of the Data Controller on his/her own message board. You can subscribe to the newsletter by clicking on
The provisions under "Newsletter and Direct Marketing" apply. When using Facebook Sweepstakes, the data handling is as described in the "Privacy aspects of sweepstakes".

In case of a reservation, the guest will be automatically redirected to the website of the Data Controller.
The Data Controller also publishes pictures/movies on its Facebook page of various events/hotels/restaurants etc. Unless it is a mass shooting, the Data Controller always asks for the written consent of the data subject before publishing the pictures.

For information about the Facebook Page's privacy practices, please see the Privacy Policy and Guidelines on the Facebook website at www.facebook.com.

XVII. PRIVACY ASPECTS OF SWEEPSTAKES

The Data Controller, alone or in conjunction with others, occasionally organises a prize draw to promote the services of a particular hotel/hotels.

The legal basis for the processing of the data in the context of the competition is the voluntary consent of the Data Subject.

The purpose of the data processing in connection with prize draws is to register the person participating in the prize draw (the Data Subject), to maintain contact and to select the winner.

Participation in the competition is possible on paper or online by registering on the Controller's websites or facebook pages, after providing the following data:

- the name of the Data Subject;
- the place of residence/residence of the Data Subject;
- the email address of the Data Subject;
- the telephone number of the Data Subject;
- the mobile phone number of the Data Subject.

The identity of the winner will be made public by the competition organiser. In doing so, the Data Controller will publish the following data:

Name of the
winner Prize

In case the delivery of the prize requires additional data processing (e.g. bank details, etc.), the Data Controller will contact the winner. The provision by the Winner of the data necessary to complete the prize constitutes consent to the processing of the data.

The data processing lasts until the end of the competition, and within 15 working days after the end of the competition, the data processed in this way (with the exception of the winner) will be deleted. The Data Controller will store the winner's data for a period of time in accordance with the applicable tax and accounting regulations and will delete them after the expiry of the time limit.

XVIII. CAMERA SURVEILLANCE AWARENESS SIGN

1. GENERAL RULES

The Data Controller uses a camera system at its premises at Debreceni út 6, 4200 Hajdúszoboszló, for the purpose of protection of property, human life and physical integrity. The legal basis for data processing is the voluntary consent of the data subject given on the basis of this information.

Consent may also be given by impulse, in particular where a natural person (the Data Subject) enters the area despite a notice posted in a public area of private property, unless the circumstances clearly indicate otherwise.

The camera system is operated by the Data Controller.

The maximum storage time for recorded footage is 3 working days. If a security incident warrants it, the recordings will be kept separately.

The cameras do not record sound. c

The location of each camera is indicated in the annex on the website.

Only authorised persons are allowed to view the recordings made by the cameras. The Data Controller's IT department is authorised to monitor the cameras.

The recordings from the cameras are stored locally at 4200 Hajdúszoboszló, Debreceni út 6, on a dedicated server. The Data Controller will take all necessary measures to avoid unauthorized access to the recordings, the Data Controller will protect the recordings by setting the IT rights. The server is equipped with virus protection and a firewall.

The Data Controller may transfer the records to law enforcement authorities upon request.

Data subjects may request information about the records, and may access the records relating to them within the retention period. In addition, data subjects have the right to object to the processing of their data, to request the erasure of their personal data and to request the restriction of processing. Data subjects may exercise their rights by making a written request to the Data Controller. The Controller shall examine the request within 30 days, decide whether it is justified and notify the data subject of its acceptance or refusal.
In addition, the data subjects may appeal to the National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/c.; www.naih.hu) and to the courts against data processing that they consider to be harmful.

2. GENERAL ALERT FROM CAMERA SURVEILLANCE

XIX. SUBMIT LAP

When using certain hotel services, the guest (Data Subject) fills in a hotel registration form, which, by providing it to the Data Controller's staff, gives his/her consent to the Data Controller to process the following mandatory data for the purposes of fulfilling its obligations under the applicable legislation (in particular the legislation on tourism and tourist tax), for as long as the competent authority is able to verify compliance with the obligations under the legislation:

- address;
- first name;
- surname;
- place and date of birth;
- citizenship;
- permanent address;
- an identity document;

The processing of the following data on third-country nationals is required by law:

- in addition to natural person identification data
- the identification data of the travel document (passport)
- address of accommodation, start and end dates of use of the accommodation
- visa
- residence permit number
- date of entry, place of entry

The provision of the mandatory data by the Guest is a condition of the use of the hotel service.

By signing and submitting the registration form, the guest consents to the processing and archiving of the personal data indicated on the registration form for the necessary period of time by the Data Controller in order to exercise its rights and fulfil its obligations.

XX. MEASURES APPLICABLE TO DATA PROCESSING

Users of the information technology systems operated by the Data Controller and persons who otherwise come into contact with personal data must comply with the following provisions in order to protect personal data.
Documents containing personal data generated in the course of work/performance of a task may only be opened on the computer equipment used for the work.

Employees must keep the access codes of the work/task equipment confidential.

In the case of correspondence sent to mobile phones for work/duty purposes and containing personal data, the document should preferably only be opened on a desktop or notebook computer. If opening via mobile phone is required, the local copy from the mobile phone must be deleted in all cases.

Mobile phones used for work/task performance, which also contain personal data processed or handled by the Data Controller, must always be used with the built-in graphic or code protection.

In the case of notebooks and other workstations provided for the purpose of work/task provision, the devices may only be used by the users and not by their relatives or other persons.

Paper-based working documents, when their use is no longer necessary, must be destroyed (e.g. by shredding) in such a way that their contents cannot be identified after destruction.

In the event of termination of employment, assignment or other legal relationship for the performance of duties, the employee shall return to the Data Controller all paper and electronic documents and data containing personal data before the last day of his/her employment, and shall not keep copies thereof.

It is prohibited to store personal data processed or handled by the Data Controller on a device for private use, unless the storage is indispensable for the performance of the work and the storage is terminated after the performance of the work.

Each employee must use the work area he or she uses in such a way that, as far as possible, documents containing personal data that are handled or processed by the Data Controller are not freely accessible. Such measures include, in particular: password protection of computer equipment, locking of the office space, placing documents in a secure place.

Personal data may only be transferred to another person using a secure communication channel or an appropriate encryption solution. Until otherwise indicated, the flow of data within the Controller's internal mail system shall be considered as a secure delivery channel. When transmitting data externally, care must be taken to ensure that the personal data is encrypted by using an SSL connection or unique encryption (e.g. MD5 encryption), by sending the password via a separate channel (e.g. SMS) and by sending it on paper via a sealed envelope.
If the Data Controller receives personal data from another Data Controller with a provision relating to the data, all users who come into contact with the data are obliged to take into account the provisions of the data controller.

In the event of a transfer of personal data, all the information necessary for keeping the data transfer register set out in the Annex to these Rules shall be sent to the Data Protection Officer by electronic mail within 3 working days.

Personal data may not be disclosed to an outside party without a confidentiality agreement.

XXI. DATA MANAGEMENT DESIGN

When new activities involving the processing of personal data are introduced, the following tasks must be carried out by the person responsible for data protection:

a) must specify

1. the scope of the personal data to be processed,

2. the purposes for which the data are processed,

3. the legal basis for the processing,

4. the duration of the processing,

b) assess the IT system in which the data will be managed, the IT system in which the data will be displayed,

c) must specify who foreseeably needs access to the data inside and outside the Controller,

d) it must be shown whether the data need to be transmitted to another person,

e) it must be indicated whether a data processor will be used for the processing, if so, what the data processor's tasks will be, and who the data processor is expected to be,

f) specify the envisaged starting date of the processing, the method and the exact location of the data collection (e.g. internet platform or paper collection).

On the basis of the established data management plan, the person responsible for data protection prepares the information notice and the final data processing contract.

XXII. AUTOMATED PROCESSING OF PERSONAL DATA

When processing personal data by automated means, the controller and the processor shall take additional measures to ensure that.

a) prevent unauthorised data entry;

b) preventing the use of automated data processing systems by unauthorised persons using data transmission equipment;

c) the verifiability and ascertainability of the bodies to which personal data have been or may be transmitted using data transmission equipment;

d) the verifiability and ascertainability of which personal data have been entered into automated data processing systems, when and by whom;

e) the recoverability of the installed systems in the event of a failure, and

f) that errors in automated processing are reported.

The Data Controller and the Data Processor acknowledge that they must take into account the state of the art when defining and implementing measures to ensure the security of the data. They shall choose among several possible processing solutions the one which ensures a higher level of protection of personal data, unless this would impose a disproportionate burden on the controller.

XXIII. MANDATORY CONTENT ELEMENTS OF DATA PROCESSING CONTRACTS

Any data processing contract concluded after the entry into force of the Code shall provide at least for:

a) the subject of a contract,

b) the data of the Controller and the Processor

c) an indication of the scope of the data processed,

d) the purposes of the processing,

e) the duration of data processing,

f) the estimated amount of personal data to be processed,

g) description and essential elements of the technical operations carried out by the processor;

h) the range of stakeholders,

i) a precise description of the tasks to be performed by the processor,

j) the fact of being bound by the instruction,

k) the obligation to provide information,

l) that the data processor is prepared for the security procedures (pseudonymisation, encryption) applied in the Regulation and that he/she implements them at the latest from the date of application of the Regulation;

m) Contact details of the Data Controller's administrator, information security officer and data protection officer,

n) the processor's confidentiality obligations,

o) the definition of appropriate technical and organisational measures, taking into account the nature of the processing, and the definition of data security requirements;

p) specifying which of the Controller's policies the processor must comply with,

q) the possibility of engaging an additional processor, if known, with an indication of the identity of the additional processor, if not known the provisions on the procedure for engagement and the Controller's right to object,

r) the sub-processor must provide adequate guarantees to implement appropriate technical and organisational measures to ensure that the processing complies with the requirements of the Regulation,

s) procedures after the processing is completed (all personal data must be erased or returned to the Controller and existing copies deleted, unless EU or Member State law requires the storage of personal data,

t) the additional data processor must conclude a contract with the data processor with the same content as the original contract,

u) the principle of cooperation, i.e. that the data processor has a duty to cooperate with the Data Controller in the performance of the subject's rights,

v) the way in which instructions are given to, or communication between, the Controller and the processor,

w) the principle of responsibility, i.e. the fact that the Data Controller shall provide the Processor with all the information necessary to fulfil the obligations of the Data Controller under the Regulation,

x) the right to audit, i.e. that the processor shall facilitate audits, including on-site audits, carried out by the Controller or by another natural or legal person mandated by the Controller,

y) certain liability issues between the parties,

z) enforcement options between the parties.

XXIV. KEEPING OF DATA ASSET RECORDS

In order to ensure transparency of data processing, the data protection officer shall keep a non-public register of data assets, which shall include at least:

a) a list of the data processed by the Data Controller,

b) the IT system in which the data is processed,

c) the physical location where the data are processed and handled,

d) a description of how any transfer of data to another controller or transfer to processors will be carried out and the security measures that will be applied,

e) the types of employees or agents who may have access to the data, including persons authorised to process the data,

f) the legal basis for the processing of the data,

g) the privacy notice, or the information necessary to clearly identify it, when and to which privacy notice the processing was subject.

XXV. FINAL PROVISIONS

In the event of an amendment to the policy, the Data Controller shall publish the new policy in the same manner as for internal policies.

The Data Controller reserves the right to unilaterally amend this Privacy Policy with prior notice to the Data Subjects. The amendment will enter into force after publication on https://thermalhotelgarden.hu/adatvedelmi-szabalyzat/.

The Privacy Policy is available at: https://thermalhotelgarden.hu/adatvedelmi-szabalyzat/

The Managing Director of the Company is responsible for compliance with and enforcement of the provisions of the Code and for updating its provisions to ensure that they comply with the legislation in force. Any amendments to the Rules shall be submitted to the Company Secretary

Hajdúszoboszló, 2019.01.01.