Privacy policy

1. Introduction

Gerbeaud Gastronomy Ltd (hereinafter referred to as " **Gerbeaud** " or " **Company** ") sets out its policies and obligations regarding the protection and processing of personal data of natural persons in this policy ("**Policy**").

Persons employed by the Company are obliged to disclose personal data obtained in the course of their work in accordance with the applicable legal provisions, in particular the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 20 December 2016 on the protection of individuals 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"; hereinafter referred to as "**GDPR**") and in accordance with the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter referred to as "**the Information Act**").

Such persons shall, in the course of their activities which necessarily involve the processing of personal data, act in accordance with the provisions of this Policy, in addition to the provisions of the specific rules applicable to the activity in question, on the understanding that where the specific rules provide for a lower level of protection of personal data than this Policy, this Policy shall apply, and where the specific rules provide for a higher level of protection, the specific rules shall apply.

2. Purpose of the Code

The purpose of this Policy is to provide a framework to ensure that the data processing carried out by the Company complies with the legal requirements in force. The Policy also aims to ensure that the Company only holds personal data in accordance with the applicable legal requirements and in a lawful manner, and that the personal data processed by the Company are at the disposal of the data subjects themselves. The Policy also aims to ensure that the rights of the data subjects are not violated when personal data are processed. To this end, the Policy contains, inter alia, the principles and provisions to be taken into account and followed in the data processing activities of the Company. Gerbeaud Gastronomy Ltd, as a data controller, acknowledges the contents of this legal notice as binding upon itself, and shall take the provisions into account in all its data processing processes and activities throughout their duration.
It undertakes to ensure that all processing of data relating to its activities complies with the requirements set out in this Policy and in the applicable national legislation and European Union acts.

The data protection policy and information relating to the data processing of Gerbeaud Gasztronómia Kft. are permanently available atwww.gerbeaud.hu/adatvedelem .

Gerbeaud Gastronomy Ltd. reserves the to change this policy and the information at any time. It will of course inform its partners and employees of any changes in due time.

If you have any questions this communication, please write to us we will answer them.

Gerbeaud Gastronomy Ltd. is committed to protecting the personal data of its customers, partners and employees, and attaches great importance to respecting the right to information self-determination of its customers and employees. Gerbeaud Gastronomy Ltd. treats personal data confidentially and

take all security, technical and organisational measures to ensure the security of the data.

Gerbeaud Gastronomy Ltd. describes its data management practices below.

3. Scope of the Code

- **Scope of the Rules**

The scope of the Policy covers all the Company's processes in the course of which data processing takes place.

- **Subject matter of the Rules**

The subject matter of the Policy extends to all persons working in the Company's premises activities involve the processing of data, to persons carrying out processing activities in connection with the Company's activities who are employed or otherwise engaged in an employment or other relationship with another legal entity, and to persons carrying out outsourced activities and employees working in such activities (who are treated for the purposes of this Policy in the same way as employees of the Company and are therefore subject to the obligations arising from this Policy.) This Policy is valid until revoked.

- **Related legislation**

The company must act in accordance with the following legal in its data processing, as set out in these internal rules:

– Regulation (EC) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) No 95/46/EC (General Data Protection Regulation, hereinafter "GDPR")

– Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter referred to as the "Infotv.")

– Act V of 2013 on the Civil Code (hereinafter: Civil Code)
– Act I of 2012 on the Labour Code (hereinafter referred to as the Labour Code Act)
– Act CXXXIII of 2005 on the rules of personal and property protection and private investigation.

- Act C of 2006 on Accounting (Accounting Act);
- Act LIII of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing (Pmt.);
- Act CCXXXVII of 2007 - on Credit Institutions and Financial Undertakings (Hpt.).

4. Description of the procedure

- **Key concepts, definitions**

Terms used and defined in this Policy in accordance with the provisions of the GDPR:

- the **GDPR** (General Data Protection Regulation) is the new EU Data Protection Regulation
- **controller**: the natural or legal person, public , 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 the specific criteria for the controller's designation may also be determined by Union or Member State law;
- **processing** : any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection,

recording, classifying, structuring, storing, transforming or altering, retrieving, consulting, consulting, , disclosing, transmitting, disseminating or otherwise making available, coordinating or combining, restricting, erasing or destroying;

- **data processor**: a natural or legal person, public , agency or any other body which processes personal data on behalf of the controller;
- **personal data** : 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;
- **Special category of personal data:** within the category of personal data, the GDPR also defines a sub-category, namely the category of Special category of personal data, which requires a higher level of protection than general personal data under the GDPR. The GDPR sets out stricter conditions for processing of Special Categories of Personal Data.

Specific Personal Data includes, but is not limited to:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic data and biometric data revealing identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons.
- **Genetic data:** any personal data relating to the inherited or acquired genetic characteristics of a natural person which contain specific information about the physiology or state of health of that person and which result primarily from the analysis of a biological sample taken from that natural person;
- **Biometric data:** 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;
- **health data:** personal data relating to the physical or mental health of a natural person, data relating to health services provided to a natural person which contain information about the health of the natural person;
- **personal data of a child:** any information or data relating to a child under the age of 18. A child under the age of 16 who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person, may be identified
- **third party** : 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;
- **data subject:** any natural person who is or can be identified on the basis of personal data;
- **data subject's consent** : a voluntary, specific, informed and unequivocal indication of the data subject's wishes by which he or she declares or gives his or her consent to the

by an unambiguous act of affirmative action, signifies his or her consent to the processing of personal data concerning him or her;

- **restriction of processing** : indication of the personal data stored with a view to restricting their processing in the future;
- **pseudonymisation**: 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;
- **profiling:** 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;
- **transfer:** when the data is made available to a specified third party;
- **filing system** : a set of personal data, structured in any way, centralised, decentralised or structured according to functional or geographical criteria, which is accessible on the basis of specific criteria;
- **data breach**: 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;

    - **General data processing guidelines**

The processing of personal data must be lawful, fair and transparent for the data subject ("**lawfulness, fairness and transparency**").

Personal data should 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 ("**purpose limitation**") is not considered incompatible with the original purpose.

The purposes for which personal data are processed must be adequate, relevant and limited to is necessary ("**data minimisation**").

Personal data must be accurate and up to date. Inaccurate personal data must be deleted immediately ("**accuracy")**.

Personal data must be stored in a form which permits identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods only if the storage is for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes ("**limited storage**").

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 ("**accountability**"), by implementing appropriate technical or organisational measures.

The data protection principles apply to all information relating to an identified or identifiable natural person.

An employee of the organisation who is responsible for data processing is liable to disciplinary action, compensation, civil and criminal liability for the lawful processing of personal data. If an employee becomes aware that personal data he or she is processing is inaccurate, incomplete or out of date, he or she must correct it or have it corrected by the person responsible for recording it.

- **Responsibilities and powers**

Responsible for implementing the Policy: all employees and managers of the Company who process personal data.

The Data Protection Officer of the Company ("**Data Protection Officer**") is responsible for monitoring the implementation and maintenance of the Policy. The Data Protection Officer also supports all employees and managers of the Company who process personal data in the organisational and professional fulfilment of data protection requirements.

- **Status and responsibilities of the Data Protection Officer**

The Company's employee is obliged to notify the Data Protection Officer if he/she becomes aware that the rules on data processing have been breached or that is a risk of such a breach. This notification must specify the data subject concerned and the person or process where or whose activities are in breach of, or threaten to be in breach of, the data protection rules.

If an employee of the Company is in doubt as to whether a procedure or activity violates the data protection rules, or if the present policy does not contain rules on the given issue, he/she is obliged to consult the Company's Data Protection Officer and ask for his/her opinion. Pending such resolution, the procedure or activity in question may not be continued or carried out. A Company employee must act in accordance with the Privacy Officer's position or guidance, even if it is issued by the Privacy Officer in connection with a specific issue or matter or if it is published as a general guidance.

Breaches of data protection rules may lead to liability or consequences under employment law (e.g. termination of employment).

The Data Protection Officer's duties include in particular:

– contributes to and assists in making decisions regarding data management and ensuring the rights of data subjects;

– monitor compliance with the provisions of this Act and other legislation on data processing, internal data protection and data security policies and data security requirements;

– investigate the notifications it receives and, if it detects unauthorised processing, request the controller or processor to cease it;

– prepare an internal privacy and data security policy;

– keeps internal data protection records;

– ensure data protection education

5. Rules applicable to data controller, data processor

◦ Accrual of Data Controller - Data Processor

The controller may be a natural person, a legal person, public authority, an agency or any other body. A processor may also be a natural person, legal person, public authority, agency or any other body, but it must be a separate person or entity from the Controller.

The Controller (alone or jointly with others) determines the purposes and means of the processing of Personal Data. The Processor may not determine them.

The Data Controller always on its own behalf, the Processor acts on behalf of the Data Controller.

The Data Controller shall act in accordance with its own decisions, the Processor shall in accordance with the instructions of the Data Controller (unless EU or Member State law applicable to the Processor also requires the Processor to process data), the Processor shall not perform logical operations on the Personal Data.

◦ Tasks of the Data Controller

The Data Controller must implement appropriate technical and organisational measures to ensure and demonstrate (see the accountability principle) that the processing of personal data is carried out in accordance with the GDPR, taking into account the nature, scope, context and purposes of the processing and the varying likelihood and severity of the risk to the rights and freedoms of natural persons.

Such measures include:

- the use of internal data protection rules (which is a broader category than the creation of an internal data protection policy);
- prepare an impact assessment before starting new data processing operations likely to present a high risk;
- consistent enforcement of the principles of data protection by default and by design;
- proper data breach management;
- positioning of the DPO (specialised area or person) in the organisation, ensuring conflict of interest, independence, etc.

These measures should be reviewed and updated at least annually.

◦ Use of a data processor

If the Data Controller a Data Processor for the processing of personal data, the Data Processor must be a person who or which.

- provides appropriate safeguards to ensure that data processing complies with the requirements of the GDPR;
- is capable of implementing appropriate technical and organisational measures to ensure the protection of the rights of data subjects and provides adequate safeguards for their implementation.

The Processor may use an additional processor, subject to the prior and written authorisation of the controller, on a case-by-case or general basis.

In the case of a general written authorisation, the Processor shall inform the Controller of any planned changes concerning the use or replacement of additional processors, thereby ensuring that the Controller has right to object to such changes.

The Data Controller is for the activities of the Data Processor. The Data Controller shall be fully responsible for the activities of any other Data Processor. The obligations of the additional Processor shall be the same as those of the Processor contracted by the Controller.

Where the Company is a processor in relation to a processing operation under this Clause, the provisions set out in relation to the processor shall apply to the Company accordingly.

6. Possible legal basis for processing

The Company may process data on the following legal bases:

- **Data subject's consent** : the Data Subject may give his or her voluntary, specific, explicit, informed and unambiguous consent, by means of a declaration or an act unambiguously expressing his or her confirmation, to the processing of his or her personal data for one or more specific purposes.

Where processing is based on consent, the controller must be able to demonstrate that the Data Subject has consented to the processing of his or her personal data.

Where the data subject his or her consent in a written statement which also relates to other matters, the request for consent must be presented in a manner clearly distinguishable from those other matters, in an intelligible and easily accessible form, in clear and plain language. The consent of the data subject shall be clearly distinguishable in relation to each individual case.

Any part of the consent form that is in breach of the provisions of the GDPR is invalid. The Data Subject has the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of the processing based on consent prior to its withdrawal. The data subject must be informed of this before consent is given. The withdrawal of consent shall be made possible in the same simple manner as the giving of consent.

- **Performance of a contract** : processing may be based on a legal basis for the performance of a contract where the processing is necessary for the performance of a contract to which the data subject is a party is necessary for the purposes of taking steps at the request of the data subject prior to entering into the contract.
- **Compliance with a legal obligation**: processing in compliance with a legal obligation may be based on a legal basis if the processing is necessary for compliance with a legal obligation to which the controller is subject. Legal obligation is understood to mean EU or Member State legal provisions.
- **Legitimate interest:** the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

Before determining whether processing is based on legitimate interest, the **so-called balancing of interests test** should be carried out, which involves first identifying the legitimate interest of the controller or third party, the data subject's interest as a counterweight and the fundamental right of the data subject, and finally, on the basis of the balancing, determining whether the personal data can be processed.

Legitimate interest, and thus on the basis of a balancing of interests, Personal Data may processed without the separate consent of the Data Subject and, inter alia, following the withdrawal of consent, under the following conditions: the processing is based on a legal authorisation of the controller; or the processing is based on a legitimate interest of the controller or a third party; or the processing is based on a legitimate interest of the data subject.

interest, provided that it has been established that the pursuit of that interest is necessary for the protection of personal data

- **Vital interest:** processing is carried out to protect the life of the data subject or the vital interests of another natural person. Personal data may be processed on the basis of the vital interests of another natural person only if there is no other legal basis for the processing in question (e.g. processing on the basis of a vital interest may be carried out in the case of humanitarian disasters, including where necessary for the monitoring of epidemics and their spread).
- **Processing in the public interest**: processing may be based on a legal ground relating to the public interest if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

7. Rules on the processing of personal data of children

The processing of personal data in relation to information society services offered directly to children is lawful when the child is at least 16 years old. In the case of children under the age of 16, the processing of personal data of children is lawful only if and to the extent that consent has been given or authorised by the person having parental authority over the child or the processing is required by law or is necessary to protect the legitimate interests of the child.

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

Given that children need special protection, all information and communications relating to the processing of personal data that is specifically relevant to children should be in clear and plain language that the child can easily understand.

This specific protection should apply in particular to the use of children's personal data for marketing purposes or for the purpose of creating personal or user profiles, and to the collection of children's personal data in the course of the use of services provided directly to them. In the case of prevention and counselling services provided directly to the child, the consent of the holder of parental responsibility is not required.

8. Processing of special categories of personal data

The concept of sensitive data is not defined in general terms in the GDPR, but only certain categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data and biometric data for the purpose of uniquely identifying natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons) are mentioned or defined separately.

As a rule, the processing of sensitive data is prohibited!

In comparison, the GDPR out exceptions, so that specific data can **be** processed despite the general prohibition if:

- the data subject has given his or her explicit consent to the processing of those personal data for the specified purposes and there is no prohibition on giving consent under Union or Member State law;
- the processing of the data is the result of obligations imposed on the controller or the data subject by legal provisions governing employment and social security and social protection

is necessary for the performance and exercise of his or her specific rights, if Union or Member State law or a collective agreement under national law, which also provides for adequate safeguards to protect the fundamental rights and interests of the data subject, so permits;

- the processing is necessary for the protection of the vital interests of the data subject, provided that the data subject is physically or legally incapacitated and is unable to give his or her consent;
- the processing relates to personal data which have been explicitly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims;
- processing is necessary for a substantial public interest, on the basis of Union or Member State law, which is proportionate to the aim pursued, respects the essential content of the right to the protection of personal data and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject;
- processing is necessary for preventive health or occupational health purposes, to assess an employee's ability to work, to make a medical diagnosis, to provide health or social care or treatment or to manage health or social care systems and services, under EU or Member State law or under a contract with a health professional;
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes on the basis of Union or Member State law which is proportionate to the aim pursued, respects the essential content of the right to the protection of personal data and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject;

Special Personal Data is processed by the Company in a different way from Personal Data. Thus, the Company controls the protection of Special Personal Data through special access rights settings, and stores it logically separate from Personal Data.

Only the head of the workplace is entitled to process the special data of employees, while the employees acting in connection with the performance of the contract are entitled to process the special data of partners, customers, guests, with the proviso that Gerbeaud Ltd will delete the special data immediately upon request after the performance of the contract.

9. Data management

The company only records personal data that the data subject voluntarily provides. By providing his/her personal data, the data subject consents to the inclusion of his/her personal data in the database of the Data Controller in accordance with this Policy.

The Company carries out the following data processing:

-

- **Recording of reservations** : In the case of reservations made by telephone, e-mail, through our online reservation system or in person, the company processes the following personal data of the Data Subjects for the purpose of identification and recording of reservations:

(1) the name of the person concerned;

(2) the e-mail address of the data subject;

(3) the telephone number of the person concerned;

(4) other personal data provided by the data subject in the "Comments" box or otherwise

(5) information on food allergies or food sensitivities;

(6) The IP address of the computer of the data subject when visiting the websites www.gerbeaud.hu, www. onyxretaurant.hu, and www.emile.hu; data about the data subject's activity on the website (e.g. tracking the number of banner clicks, login location and duration, server data, cookies).

Legal basis for processing: with regard to personal data under (1) to (4), Article 6 GDPR (1)(b) for the purposes of the performance of a contract; whereas with regard to the personal data under point (5), the Company processes the personal data under Article 9(2)(a) of the GDPR on the basis of the explicit consent of the data subject, and the personal data under point (6) for the purposes of the Company's interests under Article 6(1)(f) of the GDPR.

The processing of data for the purpose of making a reservation lasts until the fulfilment of the reservation agreement under the GTC, but no later than 90 days after the day of the reservation.

- **Newsletter subscription** : The Company sends a newsletter to inform you of its current offers.

The Company processes the following data of the data subject in connection with the processing:

(1) the name of the person concerned;

(2) the e-mail address of the data subject.

Legal basis for processing: consent of the data subject pursuant to Article 6(1)(a) GDPR GDPR.

The processing of the data provided when subscribing to the newsletter lasts until the data subject unsubscribes from the newsletter, but at the latest until the data subject withdraws his or her consent to the processing.

- **Use of services, purchase of products:** in connection with the Data Management, the Company processes the following data of the data subject:

(1) the name of the person concerned in some cases;

(2) where applicable, the details of the credit card of the person concerned;

(3) the signature of the person concerned in some cases.

(4) in the case of an invoice request, other information necessary to issue an invoice in accordance with the applicable legislation (e.g. the address of the person concerned).

Legal basis for processing: the Company processes personal data for the purpose of performing a contract pursuant to Article 6(1)(b) the GDPR.

The processing of data relating to the use of the company's services and the purchase of its products shall continue until 90 days after the termination of the contract between the data subject and the company or until the fulfilment of the legal obligations of the company.

- **When the employment relationship is established and during and in connection with the employment relationship, the company, as an employer, processes the following personal data:**

personal ig., address-, tax-, tax card, social security card, exit papers from previous job, bank account agreement, certificate - highest education and professional qualification (compulsory from 2016!), valid lung screening report (not older than 1 year), social security book, family benefit entitlement, declaration of debt, private pension fund membership certificate, declaration of membership maintenance (if membership is maintained) , salary, working hours, sick leave, training, employee events

pensioner: certificate of pension payment (date of retirement) temporary

agency worker: name, tax number or address

The Data Controller shall interpret and apply the data protection provisions with regard to labour data processing in accordance with the provisions of the Labour Code and other specific labour law rules. In addition to the general provisions of this Policy, the provisions of internal regulations and documents (e.g. personal data processing information) on labour matters shall also apply to labour-related data processing. Some specific provisions on labour-related data processing may also be contained in other relevant policies (e.g. rules on the use of mobile devices provided by the employer for personal use, rules on the use of electronic mail, e-mail filtering, employee screening).

Employees' personal data may only be processed for a specific purpose, in connection with the establishment, performance (maintenance) or termination of the employment relationship. New employees must be informed in writing, in a clear and detailed manner, on the day they start work, of all the facts relating to the processing of their data, in particular the purposes and legal basis of the processing, the identity of the controller and processor, the duration of the processing and the persons who may have access to the data.

Legal basis for processing: the Company processes the employees' data for the purposes of the performance of a contract pursuant to Article 6(1)(b) of the GDPR.

The duration of data processing arising from or related to the employment relationship lasts until the termination of the employment relationship or until the employer has fulfilled its legal obligations.

- **Job applications, CVs**

The Data Controller shall process the data it has obtained in connection with job applications solely for the purposes related to the job application and for the purpose of its assessment. The legal basis for the processing is the voluntary consent of the Data Subject, which may be withdrawn at any time by unilateral legal declaration. The personal data contained in the documents sent in connection with the job application may be known by Gerbeaud Gastronomy Ltd as the data controller or by its competent staff, agents and processors who may be involved in the assessment of the application.

The Company's HR manager will process any specific data that come to the Company's knowledge in the course of job applications solely for the purposes related to the job application and for the purpose of its assessment.

With regard to the processing of applications for employment and CVs, the provisions of the Controller's employment regulations and other documents shall apply.

10. Information

- **General requirements**

The information provided to the data subject must be concise, transparent, comprehensible and easily accessible. It must be in writing or otherwise in a clear and comprehensible form, in particular for any information addressed to children. For accountability (evidential purposes), written form is recommended.

- **Information if the Personal Data originates from the Data Subject (prior information)** If the Personal Data originates from the Data Subject, the Company as Data Controller is obliged to provide the Data Subject with the following information at the time of obtaining the Personal Data (prior information):

- the identity and contact details of the Data Controller and, if any, of the Data Controller's representative (Data Controller's name; postal address, e-mail address, telephone number;
- the identity and contact details (name, e-mail address, telephone number) of the Data Protection Officer;
- the purpose of the intended processing (specific, precise indication, without masking the real purposes) and the legal basis for the processing;
- in the case of processing based on legitimate interests, the legitimate interests of the Controller or a third party;
- the recipients or categories of recipients of personal data, where applicable;
- the fact and guarantees of the transfer to a third country or international organisation;
- the duration of the storage of personal data or, where this is not possible, the criteria for determining that duration;
- the rights of the Data Subject to request from the Controller access to, rectification, erasure, restriction of processing of personal data concerning him or her and to object to the processing of such personal data, as well as the right to data portability;
- in the case of processing based on consent, the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority;
- 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 the personal data and the possible consequences not providing the data;
- the fact of automated decision-making (profiling), its logic, and what the consequences may be for the Data Subject.

Prior information may be waived to the extent that the Data Subject already has the information.

As regards the means of information, at the start of the processing, the information may be provided paper, electronically or orally.

A hard copy of the Privacy Notice shall be provided upon request of the customer/other data subject present in person.

- **Rights in relation to data processing**
  - **Right of access and information**

At the request of the data subject, the Data Controller shall provide information on whether the processing of his or her data is ongoing. If so, the Controller shall, in addition to providing access, inform the data subject of the categories of data processed, the purposes of the processing, the recipients or categories of recipients of the processing, the duration of the storage of the data or the criteria for determining the duration, the exercise of the rights of the data subject, the rights of the controller, the National Data Protection and Freedom of Information Authority (NAIH), the source of the data and the fact of automated decision-making, including profiling. In the event of a transfer of data outside the European Union or the European Economic Area, the data subject will also be informed of the appropriate safeguards provided in relation to the transfer.

- **Right to rectification**

The data subject shall have the right to request the Controller to correct his/her data in case of inaccuracy.

If the Personal Data processed by the Data Controller needs to be rectified, the data subject may request the rectification of the data in writing (by post or e-mail), indicating the correct data.

The data subject shall notify the Data Controller in writing (by post or e-mail) of any change in any Personal Data processed by the Data Controller without undue delay, but no later than 5 days after the change. The Controller shall be liable for any damage caused by failure to give such notification or by delay in giving such notification.

- **Right to erasure**

The data subject shall have the right obtain from the controller the erasure of personal data relating to him or her without undue delay and the controller shall be obliged to erase personal data relating to him or her without undue delay in the cases provided for in the GDPR (Article 17).

In the event that the Controller has disclosed the Personal Data, i.e. transmitted them to third parties, the Controller shall, in the event of the exercise of the data subject's right to erasure, take reasonable steps to inform the other controllers to whom the Personal Data have been transmitted that the data subject has requested the deletion of the links to or copies or replicas of the Personal Data in question.

- **Right to restriction of processing**

The data subject shall have the right obtain from the controller, at his or her request, the restriction of processing if.

· the data subject contests the accuracy of the personal data;
· the processing is unlawful;

· the controllers no longer need the personal data for the purposes of the processing, but need them for the purposes of the exercise or defence of the data subject's rights;

· the data subject has objected to the processing.

- **Right to data portability**

The data subject shall have the right to receive the personal data concerning him or her which he or she has provided to the Controller in a structured, commonly used, machine-readable format and the right to transmit such data to another controller without hindrance from the Controller, if:

- the processing is based on consent; and
- the processing is carried out by automated means.

- **Right to object**

The data subject may object the processing of his or her personal data for direct marketing purposes. In this case, the Personal Data may no longer be processed for this purpose.

In exercising the rights listed above, the data subject has the right to contact the Data Controllers.

Contact details of the Data Controller:

Name: Gerbeaud Gastronomy Ltd.

Head office: 1051 Budapest, Vörösmarty tér 7-8.

Company registration number: 01-09-730963

Name of the registering court: Metropolitan Court of

Budapest Tax number: 13353779-2-41

Phone number: +361 429 9000

E-mailgerbeaud@gerbeaud.hu

- **Enforcement possibilities in relation to data processing**

National Authority for Data Protection and Freedom of

Information Postal address: 1530 Budapest, Pf.: 5.

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mailugyfelszolgalat@naih.hu

In the event of a breach of the data subject's rights, the data subject may take the controller to court. The court shall rule on the case out of turn. The data subject may, at his or her choice, bring the action before the competent court in the place where he or she resides or is domiciled.

11. Handling data protection incidents

A personal data breach may, in the absence of adequate and timely action, cause physical, pecuniary or non-pecuniary damage to natural persons, including loss of control over or restriction of their rights to their personal data, discrimination, identity theft or misuse, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, or other significant economic or social harm to the natural persons in question.

The Data Controller shall notify the authority of a data protection incident of which it becomes aware without undue delay, but no later than 72 hours. If the notification is not made within 72 hours, it shall be accompanied by the reasons justifying the delay.

A data protection incident does not have to be notified to the authority if the data protection incident is unlikely to pose a risk the rights and freedoms of natural persons.

If notification of the personal data breach to a public authority is required, in the notification:

1. (a) describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects and the categories and approximate number of data subjects affected by the breach;
2. (b) the name and contact details of the Data Protection Officer or other contact person who can provide further information;
3. (c) describe the likely consequences of the data breach;
   (d) describe the measures taken or envisaged by the company to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

If the personal data breach is likely to result in a high risk the rights and freedoms of natural persons, the company shall inform the data subject of the personal data breach without undue delay. The information shall clearly and plainly explain and communicate to the data subject the nature of the personal data breach:

1. (a) the name and contact details of the Data Protection Officer or other contact person who can provide further information;
   b) explain the likely consequences of the data breach;
   c) describe the measures taken or envisaged by the company to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

The data subject need not be informed if any of the following conditions are met:

1. (a) the company has implemented appropriate technical and organisational protection measures and these measures have been applied to the data affected by the personal data breach, in particular measures such as the use of encryption, which render the data unintelligible to persons not authorised to access the personal data;
2. (b) the company 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;
3. c) the information would require a disproportionate effort. In such cases, the data subject shall be informed by means of publicly disclosed information or by a similar measure ensuring that the data subject is informed in an equally effective manner.

If the company employs a data processor, the data processing contract should stipulate that the data processor must notify the company without delay of any data protection incident that occurs on its premises.

12. Data security

In particular, appropriate measures must be taken to protect the data against unauthorised access, alteration, disclosure, , erasure or destruction, accidental destruction or accidental damage and against inaccessibility resulting from changes in the technology used.

In order to protect the data files managed electronically in the registers, appropriate technical arrangements should be in place to ensure that data stored in the registers cannot be directly linked and attributed to the data subject.

When designing and implementing data security, the state of the art must be taken into account. Among several possible data processing solutions, the one which ensures a higher level of protection of personal data should be chosen, unless this would impose a disproportionate burden on the controller.

13. Education, training

The Company, as the Data Controller, shall ensure that all its executives and employees are familiar with and comply with the provisions of data protection legislation and this Policy, are aware of the data protection obligations and the purposes of data processing and, if necessary, act in accordance with the GDPR, the Infotv and this Policy.

14. Final and additional provisions

These Rules shall enter into force on 25 May 2018.

In matters not covered by the Rules, the provisions of the legislation in force shall apply. The provisions of the Code shall be applied in conjunction with the provisions of the mandatory regulations and procedures issued by the Company. The provisions of the Codes of Conduct shall not conflict with the provisions of these Rules.

The Company and its employees are obliged to act in accordance with the provisions of this Policy, to make the provisions of this Policy known to their managers, employees and other persons in employment and to comply with the provisions of this Policy.

Prepared by: the Company's Data Protection Officer.

The Company's Data Protection Officer is responsible for the maintenance of this Policy.