Basic data

Name: Gastroxperience Ltd
Address: 1051 Budapest, Október 6. Utca 22.
Company registration number:
Tax number: 13564955-2-41
E-mail: reteshaz@reteshaz.com
Phone: +36 1 428 0135

Purpose and scope of the Prospectus

Gastroxperience Ltd. processes, processes and stores the personal data obtained in the course of its activities for the purposes specified by law.

The purpose of the information notice is to set out the lawfulness of the records kept *by the Data Controller and to* ensure compliance with the constitutional principles of data protection, the right to information self-determination and data security. It also aims to set out the data protection and data management principles applied by the *Data Controller*, the *Data Controller's* data protection and data management policy, which the *Data Controller acknowledges as* binding on it.

The purpose of the information is to ensure that the activities of Gastroxperience Ltd. comply with the legal requirements on data protection in practice, to ensure the enforcement of fundamental rights to the protection of personal data as defined in the data management, and to ensure compliance with data security requirements.

Definitions of terms:

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 categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic data and biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons.

Data processing: any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, regardless of the procedure used, in particular the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

Transfer: making data available to a specified third party.

Disclosure: making the data available to anyone.

Data erasure: rendering data unrecognisable in such a way that it is no longer possible to recover it.

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.

Controller: the person who, alone or jointly with others, determines the purposes and means of the processing.

Processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Data subject: any natural person who is identified or can be identified, directly or indirectly, on the basis of personal data.

Recipient: the natural or legal person, public authority, agency or any other body, whether or not a third party, with whom or to which the personal data are disclosed.

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.

Consent of the data subject: a voluntary, specific, informed and unambiguous indication of the data subject's wishes by which he or she signifies, by a statement or by an unambiguous act of affirmation, his or her agreement to the processing of personal data concerning him or her.

Data breach: 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.

E-mail: (Electronic mail) electronic mail. The name refers to the method of writing or transmission, which is entirely electronic, using computer networks.

Internet: the Internet (Internetworking System) is a worldwide network of computer networks (known as a meta network) that spans the globe, connecting government, military, commercial, business, educational, research and other institutions, as well as individual users.

Web page, Web site, Web portal, Website: an electronic platform for displaying and communicating information, typically located on servers connected to the Internet (Web server). These pages have a unique address (link), which can be entered into a browser application to navigate to the page. The technology of Web pages allows you to jump back and forth (hypertext) between individual content elements and links.

Cookies: a program component used to provide convenience features on websites. There are two basic types. One is stored on your own computer and the other is stored on the server side, known as a session cookie. For data management purposes, the handling of the session cookie should be regulated. Websites should inform and declare to visitors the use of cookies.

Electronic newsletter: an electronic letter, transactional, promotional or other campaign information, typically generated automatically and sent by an application to the e-mail address of a subscriber to a mailing list.

Principles of data management

A Gastroxperience. Ltd. is committed to the protection of the personal data of the data subjects, and attaches the utmost importance to respecting the right of self-determination of the data subjects. The personal data recorded will be treated confidentially and in accordance with data protection legislation. In addition, it takes all technical and organisational measures to ensure the safe storage of data.

Personal data may only be processed for specific purposes, for the exercise of rights and the performance of obligations. At all stages of the processing, the purpose of the processing must be fulfilled and the collection and processing of the data must be fair and lawful.

Only personal data that is necessary for the purpose of the processing and is suitable for achieving that purpose may be processed. Personal data may only be processed to the extent and for the duration necessary to achieve the purpose.

The personal data will retain this quality during the processing as long as the relationship with the data subject can be re-established. The link with the data subject may be re-established if the controller has the technical conditions necessary for such re-establishment.

Possible legal grounds and purposes of processing

Personal data may be processed if at least one of the following conditions is met:

- the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into the contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary for the protection of the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- the processing is necessary for the purposes of the legitimate interests pursued by the controller or by 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.

Security of data processing

The *Data Controller* shall design and implement the processing operations in such a way as to ensure the protection of the privacy of data subjects when applying the law and other rules applicable to data processing.

The data controller or the data processor in the scope of his or her activities shall ensure the security of the data and shall take the technical and organisational measures and establish the procedural rules necessary to ensure the implementation of the legal requirements.

Appropriate measures must be taken to protect the data against unauthorised access, alteration, disclosure, disclosure, erasure or destruction and against accidental destruction or accidental damage and loss of access resulting from changes in the technology used.

In order to protect the electronically managed data files in the different 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.

The controller and the processor shall take into account the state of the art when defining and implementing measures to ensure the security of the data. The choice between several possible processing solutions should be made which ensure a higher level of protection of personal data, unless this would impose a disproportionate burden on the controller.

The controller and the processor shall implement appropriate technical and organisational measures, taking into account the state of the art and the cost of implementation, the nature, scope, context and purposes of the processing and the varying degrees of probability and severity of the risk to the rights and freedoms of natural persons, in order to ensure a level of data security appropriate to the level of risk, including, where appropriate:

1. the pseudonymisation and encryption of personal data;
2. the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data;
3. in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner;
4. a procedure to test, assess and evaluate regularly the effectiveness of the technical and organisational measures taken to ensure the security of processing.

The computer equipment, systems, data storage rooms and devices of Gastroxperience Ltd. are located in the premises of Gastroxperience Ltd.

To the best of Gastroxperience Ltd.'s knowledge, the state of the art and the computer equipment and systems used are protected from unauthorized access, data theft, deletion, alteration, accidental destruction or unintentional disclosure.

Gastroxperience Ltd. will ensure the protection of the data in accordance with the technical level available at the time and that the data cannot be directly linked and attributed to the data subject, unless otherwise provided by law.

In order to present and advertise its products and services, Gastroxperience Ltd. operates a web interface (website, web page, web site) belonging to its own domain name.

The storage of personal data in connection with the operation of the website:

Hosting and server provider:

Title: WP Online Hungary Kft.
Head office. II. floor 4
Tax number: 23480403-2-43
Company registration number: 01-09-967529
Representative: Tamás Osváth

WP Online Hungary Ltd. stores the data, it is not entitled to process them.

The *Data Controller* declares that it has implemented appropriate security measures to protect personal data against unauthorised access, alteration, disclosure, transmission, disclosure, deletion or destruction, accidental destruction or accidental damage and against inaccessibility resulting from changes in the technology used.

Information about the use of cookies

What is a cookie?

The *Data Controller* uses so-called cookies when you visit the website. A cookie is a set of letters and numbers that our website sends to your browser to save certain settings, facilitate the use of our website and help us to collect some relevant statistical information about our visitors. Cookies do not contain any personal information and are not used to identify an individual user. Cookies often contain a unique identifier - a secret, randomly generated sequence of numbers - that is stored on your device. Some cookies are deleted after you close the website, and some are stored on your computer for a longer period of time.

Legal background and legal basis for cookies:

Data processing is based on the provisions of the General Data Protection Regulation (GDPR), Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (Infotv.) and Act CVIII of 2001 on certain aspects of electronic commerce services and information society services. The legal basis for data processing is Article 6 (1) (f) of the GDPR in the case of session cookies, Article 6 (1) (a) of the GDPR in the case of other cookies and the provisions of the Infotv. Article 5(1)(a) of the GDPR.

Main features of the cookies used by the website:

Session cookie: these cookies are temporarily activated while you are browsing. These are activated temporarily from the moment the browser window is opened until the moment it is closed. Once the browser is closed, all session cookies are deleted. No personal data is stored in session cookies.

The site uses the following cookies necessary for its operation: PHPSESSID, _hssrc
Purpose: to record the user's status during browsing

Security cookie: security cookies are used to authenticate users, prevent misuse of login information and to protect user data from unauthorised persons.

Google Adwords cookie: when someone visits our site, the visitor's cookie ID is added to our remarketing list. Google uses cookies - such as NID and SID cookies - to personalise the ads you see in Google products, such as Google Search. It uses such cookies, for example, to remember your recent searches, your previous interactions with advertisements from individual advertisers or search results, and your visits to advertisers' websites. The AdWords conversion tracking feature uses cookies. To track ad sales and other conversions, cookies are saved on a user's computer when they click on an ad. Some common uses of cookies include: selecting ads based on what is relevant to a particular user, improving campaign performance reporting, and avoiding displaying ads that the user has already viewed (Processor: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.)

Google Analytics cookie: Google Analytics is Google's analytics tool that helps website and application owners to get a more accurate picture of their visitors' activities. The service may use cookies to collect information and report statistics about website usage without individually identifying visitors to Google. The main cookie used by Google Analytics is the "__ga, _gat, _gid" cookie. In addition to generating reports on website usage statistics, Google Analytics, together with some of the advertising cookies described above, may also be used to display more relevant ads in Google products (such as Google Search) and across the web (data processor: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.)

This is done in order to align the ads displayed to the user across devices and to measure conversion events. These cookies are stored on google.com/ads, google.com/ads/measurement or googleadservices.com. If you do not want ads to be displayed in a coordinated, cross-device manner, you can turn off ad personalization by using the Ads Settings.

Facebook pixel (Facebook cookie): a Facebook pixel is code that allows the website to report conversions, create audiences and provide the site owner with detailed analytics on how visitors use the site. The Facebook remarketing pixel tracking code is used to display personalised offers and ads to website visitors on Facebook. The Facebook remarketing list is not suitable for personal identification (fr, tr).
For more information about the Facebook Pixel / Facebook Wallpaper, please visit: https://www.facebook.com/business/help/651294705016616
(Data Processor: Facebook Inc., 1 Hacker Way, Menlo Park, California 94025, USA, Phone: +1 650-543-4800.)

You can delete cookies set by www.reteshaz.com from your device at any time using your browser. For details on how to delete or manage cookies, please refer to the help section of your browser. You can also use your browser to block cookies or request a notification each time your browser receives a new cookie. Blocking cookies may technically prevent you from using our website.

If you do not accept the use of cookies, certain features will not be available to you. For more information on how to delete cookies, please click on the links below:

InternetExplorer: http://windows.microsoft.com/en-us/internet-explorer/delete-manage-cookies#ie=ie-11

Firefox: https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer

Chrome: https://support.google.com/chrome/answer/95647?hl=en
Edge: Settings -> Advanced settings -> Cookies ("Enable cookies" / "Block all cookies" / "Block only external cookies" or F12 - Debugging - Cookies

Purpose of processing, method of processing:

The data processing is based on the voluntary, explicit consent of the users of the contents of the website www.reteshaz.com, in that the data provided by them during their visit and use of the website is used for the purpose of continuous communication between the users of the website and the data controller and for public opinion research.

The purpose of the data processing is to ensure the provision of services available under the URL of the website www.reteshaz.com, to operate an information interface, to compile statistics and to handle questions received through the website.

The storage of visitor statistics is for statistical purposes only.

The controller will not use the personal data for any purpose other than the purposes stated. The processing of the data thus provided is subject to the user's voluntary consent.

Images and videos displayed on our Facebook page

On our Facebook page, we pay special attention to ensure that the content of images and videos published on our Facebook page does not infringe the privacy rights or legitimate interests of others, and that we have permission and authorisation for their lawful use in all cases.

Purpose of the processing:

To inform visitors to our Facebook page.

Legal basis for processing:

The legal basis for the processing is the voluntary consent of the data subject pursuant to Article 6 (1) (a) of the General Data Protection Regulation (GDPR) and Section 2:48 of the Civil Code.

Scope of the data processed:

Images may include identifiable, recognizable natural persons.

Duration of processing:

Until the data subject's consent is withdrawn or the content is removed from our website.
Data Processor: Facebook Ireland Limited, 4 Grand Canal Square, Grannd Canal Harbour, Dublin 2 Ireland

Gastroxperience Ltd. does not assume any responsibility for the previous pages that have been deleted but archived with the help of Internet search engines. The removal of these pages is the responsibility of the search site operator.

Images and videos displayed on our Instagram page

We take special care to ensure that the content of images and videos published on our Instagram page does not infringe the privacy rights or legitimate interests of others, and that we have permission and authorisation for their lawful use in all cases.

Purpose of the processing:

To inform visitors to our Instagram page.

Legal basis for processing:

The legal basis for the processing is the voluntary consent of the data subject pursuant to Article 6 (1) (a) of the General Data Protection Regulation (GDPR) and Section 2:48 of the Civil Code.

Scope of the data processed:

Images may include identifiable, recognizable natural persons.

Duration of processing:

Until the data subject's consent is withdrawn or the content is removed from our website.

Data Processor: Facebook Ireland Limited, 4 Grand Canal Square, Grannd Canal Harbour, Dublin 2 Ireland

Gastroxperience Ltd. does not assume any responsibility for the previous pages that have been deleted but archived with the help of Internet search engines. The removal of these pages is the responsibility of the search site operator.

Miscellaneous provisions

Only our employees are authorised to access the data you provide.

The data controller does not verify the data provided by the user, the user is solely responsible for their authenticity and correctness.

The data controller keeps all data and facts about users confidential and uses them exclusively for the development of its services and for its own research and statistics. The publication of these statements may only take place in a form that does not allow the individual identification of each user.

The data processing of www.reteshaz.com is carried out in accordance with the legal provisions in force and the data protection rules set out in this policy, and is used exclusively in the course of its activities, and is not transferred to any other natural or private person without the user's consent. The only exceptions to this rule are data disclosures based on legal obligations and the use of data in aggregate statistical form, which does not include the name or any other identifiable data of the user.

If the data controller intends to use the data provided for purposes other than those described in this Privacy Policy, the user will be duly informed of this at the e-mail address provided and his/her prior explicit consent will be obtained, and the user will be given the opportunity to prohibit the use of the data for other purposes.

In the case of data processing based on consent, we may process your data until the User prohibits it in writing to reteshaz@reteshaz.com, in which case we will delete the data from our records within 48 hours. Other data subjects' rights can be exercised using the same contact details. In case of notification of data changes, the transfer will be completed within 48 hours.

Gastroxperience Ltd. does not assume any responsibility for the previous pages that have been deleted but archived with the help of Internet search engines. The removal of these pages is the responsibility of the search site operator.

Data protection incident
The *Data Controller* declares that it has implemented appropriate security measures to protect personal data against, in particular, unauthorised access, alteration, disclosure, transmission, disclosure, erasure or destruction, accidental destruction or accidental damage and inaccessibility resulting from changes in the technology used.

The *Data Controller shall ensure that the* data it processes are accessible only to those authorised to access them, and in this context it shall also ensure the security of data processing by means of IT and work organisation measures and internal measures.

However, the *Data Controller* must also inform the data subjects of the fact that data transmissions by any means using the Internet are exposed and vulnerable to unlawful and fraudulent attacks, even when using state-of-the-art security measures, software and systems providing the best protection. The computers used by the *Data Controller's* employees and contributors are protected by a unique password and are equipped with firewalls and anti-virus software to prevent unauthorised access and intrusions.

The data controller shall notify the data protection incident to the competent supervisory authority (National Authority for Data Protection and Freedom of Information address: 1055 Budapest, Falk Miksa u. 9-11.; phone: +36-1-391-1400; e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu) without undue delay and, if possible, no later than 72 hours after the data protection incident has come to its attention, unless the data protection incident is unlikely to pose a risk to the rights and freedoms of natural persons.

The data subject does not need to be informed if any of the following is true:

- the controller has implemented appropriate technical and organisational protection measures and these measures have been applied in relation to the data concerned by the data protection incident, in particular measures such as the use of encryption, which render 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,
- information would require a disproportionate effort. In such cases, the data subjects should be informed by means of publicly disclosed information or a similar measure should be taken to ensure that the data subjects are similarly informed.

Description of rights in relation to data management:

Under Article 15 of the GDPR, the data subject may request access to personal data concerning him or her as follows:

The data subject has the right to receive feedback *from the Data Controller as to* whether or not his or her personal data are being processed and, if such processing is ongoing, the right to access the personal data and the following information:

1. a) the purposes of the processing;
2. b) the categories of personal data concerned;
3. (c) the recipients or categories of recipients to whom or which the personal data have been or will be disclosed, including in particular recipients in third countries or international organisations;
4. (d) where applicable, the envisaged duration of the storage of the personal data or, if this is not possible, the criteria for determining that duration;
5. (e) the right of the data subject to obtain from the Controller the rectification, erasure or restriction of the processing of personal data concerning him or her and to object to the processing of such personal data;
6. (f) the right to lodge a complaint with a supervisory authority;
7. (g) where the data have not been collected from the data subject, any available information on their source;
8. (h) the fact of automated decision-making, including profiling, and, at least in those cases, the logic used and clear information on the significance of such processing and its likely consequences for the data subject.

The *Data Controller* shall provide the data subject with a copy of the personal data processed. For additional copies requested by the data subject, the *Controller* may charge a reasonable fee based on administrative costs. Where the data subject has made the request by electronic means, the information shall be provided in a commonly used electronic format, unless the data subject requests otherwise. The right to request a copy should not adversely affect the rights and freedoms of others.

Pursuant to Article 16 of the GDPR, the data subject has the right to obtain from the Data Controller the rectification of personal data concerning him or her.

If the data subject so requests, the *Controller* shall correct inaccurate personal data relating to him or her without undue delay. Taking into account the purposes of the processing, the data subject shall have the right to request the completion of incomplete personal data, including by means of a supplementary declaration.

Pursuant to Article 17 of the GDPR, the data subject has the right to obtain *from the Controller the* erasure of personal data relating to him or her as follows:

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

1. (a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
2. (b) the data subject withdraws the consent on which the processing is based and there is no other legal basis for the processing;
3. (c) the data subject objects to processing for reasons of public interest, in the exercise of official authority or in the legitimate interest of the controller (third party) and there are no overriding legitimate grounds for the processing, or the data subject objects to processing for direct marketing purposes;
4. d) the personal data have been unlawfully processed;
5. (e) the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the controller is subject;
6. f) the personal data were collected in connection with the provision of information society services.

Where the *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 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 Data Subject's right to erasure may only be limited if the following exceptions in the GDPR apply, i.e. if the above grounds apply, the continued retention of personal data is considered lawful:

1. a) if the exercise of the right to freedom of expression and information, or
2. b) if compliance with a legal obligation, or

3. (c) when carrying out a task carried out in the public interest, or
4. (d) where the exercise of official authority vested in the controller, or
5. (e) where it is in the public interest in the field of public health,
6. f) for archiving purposes in the public interest, or
7. (g) for scientific and historical research or statistical purposes; or
8. h) if necessary for the establishment, exercise or defence of legal claims.

Pursuant to Article 18 of the GDPR, the data subject shall have the right to obtain *from the Controller the* restriction of the processing of personal data concerning him or her, as follows:

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

1. (a) the data subject contests the accuracy of the personal data, in which case the restriction shall apply for the period of time necessary to allow the Controller to verify the accuracy of the personal data;
2. (b) the processing is unlawful and the data subject opposes the erasure of the data and requests instead the restriction of their use;
3. (c) the controller no longer needs the personal data for the purposes of the processing, but the data subject requires them for the establishment, exercise or defence of legal claims; or
4. (d) the data subject has objected to processing in the public interest, in the exercise of official authority or in the legitimate interest of the controller (third party); 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.

Where processing is restricted on the basis of the above, 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 Data Controller shall inform the data subject at whose request the processing has been restricted in advance of the lifting of the restriction.

Pursuant to Article 21 of the GDPR, the data subject has the right to object to the processing of personal data concerning him or her by the *Controller* as follows:

The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to processing of his or her personal data in the public interest, in the exercise of official authority or in the legitimate interest of the controller (third party), including profiling based on such processing. In such a case, 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.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such purposes, including profiling, where it is related to direct marketing. If the data subject

objects to the processing of personal data for direct marketing purposes, the personal data may no longer be processed for those purposes.
The right to object must be explicitly brought to the attention of the data subject at the latest at the time of the first contact with the data subject and the information must be clearly displayed separately from any other information.

In the context of the use of information society services and by way of derogation from Directive 2002/58/EC, the data subject may exercise the right to object by automated means based on technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject shall have the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Pursuant to Article 20 of the GDPR, the data subject has the right to the portability of personal data concerning him or her as follows:

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

1. a) where the legal basis for the processing is the consent of the Data Subject or the performance of a contract with the Data Subject
2. b) and the processing is carried out by automated means.

In exercising the right to data portability, the data subject has the right to request, where technically feasible, the direct transfer of personal data between controllers.

The exercise of the right to data portability must not prejudice the right to erasure. The right to data portability shall not apply where 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.

The right to data portability must not adversely affect the rights and freedoms of others.

Pursuant to Article 7(3) of the GDPR, the data subject has the right to withdraw his or her consent to the processing of his or her personal data at any time, as follows:
The data subject has the right to withdraw his or her consent at any time. Withdrawal of consent shall not affect the lawfulness of processing based on consent prior to its withdrawal. The right to withdraw consent is as simple as giving it.

Within five years of the death of the data subject, the rights to which the deceased person is entitled during his or her lifetime, as defined by law, may be exercised by a person authorised by the data subject by means of an administrative arrangement or a declaration in a public or private document having full probative value made with the controller.

Even if the person concerned has not made a declaration, his or her close relative under the Civil Code is still entitled to assert certain rights to which the deceased person was entitled during his or her lifetime.

Remedies

If the Data Subject believes that the *Data Controller* has violated a legal provision on data processing or has failed to comply with a request, he or she may initiate proceedings with the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa u. 9-11., postal address: 1363 Budapest, PO Box 9., telephone: +36 (1) 391-1400, fax: +36 (1) 391-1410, e-mail: ugyfelszolgalat@naih.hu, URL: http://naih.hu) to have the alleged unlawful processing terminated.
The *Data Subject* may also take the *Data Controller to* court in the event of a breach of his or her rights or if the *Data Controller* has not complied with a request. The court shall rule on the matter out of turn. The *Data Controller* shall have the burden of proving that the processing is lawful. The tribunal shall have jurisdiction to rule on the action. The *Data Subject* may, at his or her option, bring the action before the competent court of his or her place of residence or domicile. A person who otherwise lacks legal capacity may also be a party to the proceedings. The National Authority for Data Protection and Freedom of Information may intervene in the lawsuit in order to ensure that the *Data Subject* is successful.

If the court grants the application, the controller or processor shall be required to.

- to stop unlawful processing operations,
- to restore the lawfulness of the processing,
- engage in specified conduct to ensure the exercise of the rights of the data subject,
- if necessary, also decide on the claim for damages and compensation.

If, in connection with the Gastroxperience Ltd. Facebook page, you become aware that the legal provisions on data processing have been violated or that a request has not been fulfilled, your personal data will be processed by Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. The Irish Data Protection Authority has the power to act on this matter, so you should take your complaint to the Irish Data Protection Commission (21 Fitzwilliam Square, South Dublin 2, D02 RD28, Ireland).

Data Transfer Statement – Simplepay

I acknowledge the following personal data stored in the user account of Gastroxperience Ltd. (1051 Budapest, Október 6. Utca 22.) in the user database of reteshaz.com
will be handed over to OTP Mobil Ltd. and is trusted as data processor. The data transferred by the data controller are the following:
[data transmitted by the trader]

The nature and purpose of the data processing activity performed by the data processor in the SimplePay Privacy Policy can be found at the following link:
https://simplepay.hu/adatkezelesi-tajekoztatok/