

PRIVACY POLICY
OF
LEO BISTRO AND ROOFTOP
AND
WWW.LEOBUDAPEST.HU
WEB PAGE

Budapest, 25. November, 2021

Table of contents

INTRODUCTION	3
I. TITLE OF CONTROLLER	4
II. DATA PROCESSING	4
II.1. Processing personal data for table reservation purposes at the Restaurant.....	4
II.2. Processing personal data for sending out newsletters.....	5
II.3. Processing data for protection of property	7
III. DATA SECURITY	7
III.1. Operational provisions.....	7
III.2. Technical provisions.....	7
IV. YOUR RIGHTS	8
IV.1. Revoking your consent.....	8
IV.2. Access	8
IV.3. Rectification.....	9
IV.4. Erasure	9
IV.5. Restriction.....	9
IV.6. Data portability.....	10
IV.7. Objection	10
IV.8. Application procedures related to the exercise of rights.....	10
V. YOUR JUDICIAL REMEDIES	11
V.1. Complaints to the National Authority for Data Protection and Freedom of Information	11
V.2. Judicial proceedings	11
1. attachment	12
2. attachment	13
3. attachment	15

INTRODUCTION

Present Privacy Policy (**Policy**) provides **information** on the operations of Beefbar Budapest (**Restaurant**), located at 1013 Budapest, Clark Ádám tér 1., operated by Leo Restaurants Kft (**Controller**), and its **data processing** policies linked to the website <http://budapest.beefbar.com>

The Policy was prepared in compliance with legislation relevant to the GDPR, the Infotv, as well as to the function of the surveillance system. The list of the legislation is included in the **attachment 1**.

The Policy regarding the data processing of surveillance systems operating on the premises of the Controller is in effect starting 25. November of 2021 until countermanded. The Policy may be obtained in printed form at the Restaurant and is available on the following URL.

The Controller reserves the right to change present Policy at anytime unilaterally. In the event the Policy should change, we will notify our guests on the premise.

Budapest, 25 November,2021

Leo Restaurants Kft.

I. TITLE OF CONTROLLER

The Policy outlines the title and the contact information of the **Controller**. The titles and contact details of the **Data Processors** are included in **attachment 2.** of the Policy.

Title of Controller: Leo Restaurants Kereskedelmi és Szolgáltató Korlátolt

Felelősségű Társaság

Shortened title: Leo Restaurants Kft.

Headquarters: 1036 Budapest, Lajos utca

48. B/4.

31. Company registration number:

01-09-950822

Tax number: 23055348-2-41

E-mail: info@leobudapest.hu

II. DATA PROCESSING

1. Processing personal data for table reservation purposes at the Restaurant.

Controller allows guests to make table reservations at the Restaurant directly via telephone, electronic mail, and through the Website. Within this framework, your personal data will be processed as the following:

- Areas of personal data processed: family – and surname, email address, phone number, number of guests, date of table reservation, time of table reservations
- Object of Data Processing: table reservation on the premises of the Restaurant operated by the Controller
- Claim of Data Processing: consent of the affected person in accordance with (GDPR 6. (1) a)
- The period for which the personal data will be processed: end of table reservation or the commencement of obligatory erasure (revocation of consent, practicing the right to object or erasure to processing data)

Personal data collected with the intention to use for making a table reservation will be accessed primarily by the Controller, and by Open Table Ltd the operator of the table reservation system. The Controller will not disclose personal data managed to any third party – with headquarters in Hungary, any European or Third World country. The personal data may be disclosed to the competent authorities as authorized by the applicable laws in case of any legal procedure by court or any other authorities.

You may exercise your right to: revoke your consent, access your personal data, rectification erasure, restrict processing, data portability, and your right to object to processing personal data collected with the intention to make a table reservation. The conditions to exercise any of these rights are laid out in **chapter IV.** of the Policy.

2. Processing personal data for sending out newsletters.

Should you wish to receive up to date information about our latest news and promotions, you may sign up to our online newsletter. The newsletters are forwarded to you by the Controller using the Mailchimp services. Accordingly, your personal data will be processed as the following:

- Areas of personal data processed: email address (mandatory), family – and surname, date of birth, phone number (voluntary information)
- Object of Data Processing: sending out newsletters containing economic marketing
- Claim of Data Processing: consent (GDPR 6. (1) a).
- The period for which the personal data will be processed: until the revocation of consent or the commencement of erasure request.

Personal data collected with the intention to send you newsletters will be accessed primarily by the Controller, and the Rocket Science Group LLC as the operator of Mailchimp services. The personal data may be disclosed to and accessed by the competent authorities as authorized by the applicable laws in case of any legal procedure by court or any other authorities.

You may exercise your right to: revoke your consent, access your personal data, rectification erasure, restrict processing, data portability, and your right to object to processing personal data processed for sending you newsletters. The conditions to exercise any of these rights are laid out in **chapter IV.** of the Policy.

3. Processing data for protection of property

Information on data processing regarding the electronic surveillance system operated on the premises of the Restaurant is included in document c of the privacy policy of the surveillance system operated on the premises of Beefbar Budapest.

III. DATA SECURITY

The Controller and the processors are eligible to gain insight on your personal data only to a measure that is necessary in order to complete their tasks included in their job description. Controller shall take all necessary security, technical and operational measures to guarantee the security of data.

1. Operational provisions

The Controller enables access to IT Systems with a personally identifiable entitlements.

At the time of the allocation of entitlements, the principle of „ necessary and sufficient” applies, that is, all users are eligible to utilize the IT Systems and services of Controller only to the measures that is necessary in order to complete their tasks along with the necessary titles and limited to the time necessary to.

Access rights to the IT Systems and services may be received only by those who are not restricted due to security or other (e.g. conflict of interest) reasons, and is in possession of essential professional, business and information security know how required to the safety in use.

The Controller and the processors accept strict confidentiality by written statement and shall proceed in all their activities according to these confidentiality rules.

2. Technical provisions

The Controller stores data- except data stored by the processors- on internal private devices, in data centers. IT instruments storing data are kept by the Controller in isolated, separate, locked server room, secured by a multi-staged process in identifying entitlements and allowing access.

The Controller is protecting his internal network with multilayered, firewall security. On all access points of the applied public networks there is a hardware firewall (border protection)used at all times. The Controller stores data redundantly- that is in more than one place- in order to protect them from destruction, losses, damages and unlawful eradication in case of a fail-down of any IT devices.

We protect our internal networks with multilevel, active, complex security (virus protection) against outside invasions of harmful codes. Controller provides necessary outside access to IT systems and databases operated by the Controller via encrypted data link. (VPN).

We shall take all the effort to ensure that our IT devices and software constantly measure up to the general standards of technical solutions on the market.

We develop logging systems that allow us to control and trace operations carried out, detect recent incidents, e.g. unauthorized access.

The Controller’s server is placed on a separate, dedicated server of the hosting service provider, secured and locked.

IV. YOUR RIGHTS

The Controller finds important that data processing shall meet the requirements of fairness, legality and transparency. Accordingly, you may request information on the processing of your personal data, you may also request any of your personal information to be corrected or to be erased-with the exception of mandatory data processing-, you may revoke your consent, and you may request Our Company to transfer the data that we have collected to another organization, or directly to you, and you may exercise your right to object. In order for you to be familiar with your rights and the conditions under you may exercise them, we offer the following policy.

1. Revoking your consent

In the case of data processing based on voluntary consent, you have the right to revoke your consent at any time without any explanation. Your revocation does not affect the legality of data processed

based on consent prior the revocation. At the same time the controller will not continue use your personal data and will erase them. You may give your consent by contacting the Controller or as listed below:

2. Access

You – based on your consent to the Controller submitted on any channels- have the right to request to access your personal data that is processed by the Controller. Within this context, we offer information on the following:

- do we process your personal data
- object of data processing
- categories of affected personal information
- recipients or categories of recipients with whom your personal data was or will be shared.
- duration of storing your data targeted
- your rights
- your judicial remedies
- information on data sourcing

You may also request a copy of your personal data processed by Controller. In this case the Controller will provide the personal information in articulated, frequently used, computer friendly version (PDF/XML), and printed on paper. The request of a copy is free of charge.

3. Rectification

You have the right to request- based on your consent to the Controller submitted on any channel- that Our Company correct any information you believe is inaccurate. You also have the right to request Our Company to complete the information you believe is incomplete. Should some of the necessary data to correct inaccurate information be missing, the Controller may request to be provided with that information and proof of accuracy. Until all information necessary to complete the correction is not provided, Controller will temporarily suspend the process and use of affected personal data- except the storing.

4. Erasure

You have the right to request– based on your application submitted to the Controller on any channel- to have your personal data processed by the Controller to be erased under any of the following conditions:

- your data is not required any further
- should you have any concerns regarding our matters of legality in data processing

Should the Controller find your request to erase your personal data relevant, he shall discontinue to process the data, and shall eradicate all relevant personal data processed earlier. Besides, the obligation to delete personal data may be relevant based on the withdrawal of consent, the right to object, as well statutory obligations.

5. Restriction

You have the right to request– based on your application submitted to the Controller on any channel- to have your personal data processed by the Controller to be restricted under any of the following conditions:

- should you have any concerns regarding our matters of legality in data processing, and have the data restricted instead of being erased;
- Your data is not required any further, but You need them for civil claim establishment, exercise and defence.

The Controller shall automatically restrict personal data processing, should you contest the accuracy of the data. In this event, data is subject to restriction for a period enabling the controller to verify the accuracy of personal data.

During the period of restriction, there shall not be any type of data processing actions taken regarding the relevant data. Personal data may be processed under the restriction period only under the following conditions:

- based on the consent of subject
- in case for the establishment, exercise or defence of legal claims
- in case for the defence of any natural or legal person rights
- important public interest

You will be notified in advance of the restriction by the Controller.

6. Data portability

You have the right to request– based on your application submitted to the Controller on any channel- to have your personal data processed by the Controller to be made available in order to be used as per instructed by you. You may also request to have your personal data forwarded to any other controller appointed by you.

This right is restricted to personal data submitted by You, processed based on your voluntary consent only. Any other data may not be forwarded. Controller will provide the personal information in articulated, frequently used, computer friendly version (PDF/XML), and printed on paper.

Please be notified that by exercising this right, your personal data will not be automatically erased from the Controller s database. At the same time, You may contact the Controller again and keep contact with the Controller.

IV. 7 Objection

The contact person of a not natural person- based on the application submitted to the Controller – may object to the processing of data subject for communication purposes at any time. In this case Controller shall not process data subject for this purposes as well to erase them. Controller will examine whether there are compelling reasons or legitimate interests (eg. establishment, exercise and defence of legal claims), which will be given precedence over the interests, rights and freedoms of the data subject. Should there be such reasons or interests identified, Controller will continue process data subject. Otherwise data subject no longer can be used.

IV.8. Application procedures related to the exercise of rights

Controller shall inform you without undue delay, and at the latest within 1 month upon your application received regarding the procedures related to exercising your rights. If necessary- considering the complexity of application and the number of requests- that period may be extended. Controller shall inform you of the extension of that period setting out the reasons of the delay at the latest within 1 month of receiving your application.

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy..

The Data Manager provides information on the action or failure to form your wish. If you submitted the application electronically, the information will be entered electronically, unless you contend otherwise.

The Data Manager provides the requested information and information free of charge

The data Controller shall inform any recipient of any rectification, erasure or data-management restrictions it carries with whom or which the personal data is disclosed, unless this proves impossible or require a disproportionate effort. Your request to that effect to the Data Controller informs you of these recipients.

In order to fulfill the request, the data Controller is obliged to make sure that indeed entitled to exercise his rights. To do this - where appropriate - it may be necessary for you to appear in person for the purpose of identification Controller headquarters.

V. YOUR JUDICIAL REMEDIES

If the Data Manager, contrary to the law improperly handles your personal information, you may request to exercise the rights of the data controller is not fulfilled or inappropriate way, it may take several remedies.

1. Complaints to the National Authority for Data Protection and Freedom of Information

If you complain to the Data Management activities, file remedies and complaint to the National Authority for Data Protection and Freedom of Information on any of the following contacts:

Head office: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Postal address: 1530 Budapest, Pf. 5.

Phone number: +36-1-391-1400

Fax: +36-1-391-1410

E-mail:

ugyfelszolgalat@naih.hu Web

page: <http://www.naih.hu>

Online initiation of cases: <http://www.naih.hu/online-uegyinditas.html>

2. Judicial proceedings

In addition to the official appeals to you, you can also go to court because of the Data Management activities. Apply to the lawsuit the conditions of the GDPR, the Infotv, and the Ptk. and the Pp. The assessment of trial falls under the competence of the tribunal. The lawsuit may be brought before the tribunal of the place of residence of the subject in matter according to his or her choice. (you may find the list of tribunals and contact information on the following link: <http://birosag.hu/torvenyszekek>). Issues related to the opening of the trial, please consult a lawyer.

I. attachment

The rules concerning

In developing the Information Data Management took into account the relevant existing legislation and the relevant international recommendations, with particular regard to the following:

- the protection and the free movement of such data, and Directive 95/46 / EC and repealing the natural persons on the treatment of personal data on 2016/679 / EU of the European Parliament and of the Council (GDPR) 2016 of 27 April;
- CXII of 2011 law on Informational Self-Determination and Freedom of Information Law. Act CXII of 2011. (Infotv)
- Act C of 2003 on electronic communications;
- Act V of 2013 Civil Code (CC.);
- 2016 CXXX of Civil Procedure Law (Pp)

2. attachment

Concepts related to the management of personal data

- controller: the legal entity which determines the purposes and means of the processing of personal data;
 - data processing means any operation or set of operations with automated or non-automated means, such as collection, recording, organization, division, storage, adaptation or alteration, consultation, use, disclosure, transmission, dissemination or otherwise of personal data or files on by making available, coordination or combination, restriction, erasure or destruction;
 - Data transmission: to make specific third party to access the data;
 - data deletion: making unrecognizable in such a way that the data restoration is no longer possible;
 - Data indication: Performance data for the purpose of identifying markings to distinguish;
 - Limiting data management means the marking of stored personal data in order to limit future treatment;
 - Data destruction: destruction of all physical media containing the data;
 - Data processing: the legal entity that manages personal information on behalf of the controller;
 - Addressed: any natural or legal person, public authority, agency or any other entity with whom or with which to communicate personal data, regardless of whether a third party;
 - Cookies: small data packet positioned sent by a web server and specified in the user's computer time (text file), which depending on the signal air from the server can also be supplemented during recent visits, that is, if the browser sends back a previously saved cookies, the possibility of managing the cookie provider current visit is to connect the user to the previous ones, but only in respect of their content;
 - concerned: an identified or identifiable natural person; identify the natural person who, directly or indirectly, in particular on the basis of an identifier, such as your name, number, location data, online identifier or to one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual identified.
 - third party: the natural or legal person, public authority, agency or any other entity that is different from the data subject, the controller, the processor and the persons who are authorized to process personal data within the data controller or data processor direct control;
- the consent: the will of concerned voluntary, specific and informed and unequivocal expression with which the declaration or confirmation by the unmistakable expressive acts concerned indicate that consent to the treatment of personal data relating to him;

- IP address: all networks using TCP/IP communication protocol operate with server farms identified by IP address, that is an identification number, which allow the authentication of the given server via network. Well known, that all computers connected to the network is assigned an IP number by which it is identifiable.

- personal data: any information relating to the data subject

- protest: the statement in question, which objects to the processing of personal data and calls for the elimination of data management and data being erased.

3. *attachment*

Names and data of Processors

Name of Processor: OpenTable International Ltd.

Seat: Fourth Floor, 14-18 Finsbury Square, London EC2A 1AH

Web site: www.opentable.co.uk

Activities performed: operation of the program allowing table reservation

* * *

Name of processor: Rocket Science Group LLC

Seat: 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA

30308 USA E-mail: privacy@mailchimp.com

Web page: <https://mailchimp.com>

Activities performed: operation of MailChimp newsletter services