Public Privacy Notice of Galuschka Bistro & Garden

Please read this Notice carefully in order to understand how we process your personal data. If you have any questions, please contact us using any of the contact details provided below. You are welcome to turn to us with confidence.

As data controller, we respect the privacy of all individuals who provide us with personal data and we are committed to protecting such data.

This Notice applies equally to our customers, the employees working for our customers, visitors to our website, our guests, our business partners, our suppliers (and potential suppliers), as well as the employees of all of the above.

In the course of our operations, we engage external partners for the performance of certain tasks. In relation to these tasks, we maintain contractual relationships with such partners, and these contracts also cover the rules applicable to data processing. With these partners, we act either as joint controllers or as controller and processor, and the principles set out in this Privacy Notice apply to them accordingly. For each processing activity, this Notice specifies the name, registered office and contact details of the partner concerned.

If you wish to request any operation in relation to the processing of your personal data (such as the transfer, erasure or rectification of your data), please contact us using any of our contact details.

1. Data of the Data Controller

Name: SKDNZ Ingatlanhasznosító Kft.

Registered office: 1123 Budapest, Alkotás út 55–61, Hungary

E-mail: info@galuscha.hu

Represented by: Zsolt Bencze, Managing Director

2. Principles of Data Processing

2.1 Lawfulness, fairness and transparency

Personal data must be processed lawfully and fairly, and in a manner that is transparent to you. But what does this mean more precisely? We explain this in more detail below.

Lawfulness and fairness mean that personal data must always be obtained by lawful and fair means and that these conditions must be maintained throughout the entire period of processing. It is also necessary that there is an appropriate legal basis for the processing. The GDPR defines six legal bases on which we may process your personal data: consent, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest and the legitimate interests of the Controller. These legal bases are described in detail in the chapter entitled “Lawfulness of Processing”.

Transparency means that data processing must always be carried out in such a way that you are aware, for the entire duration of the processing, of all circumstances affecting you, for example what data we process about you, for what purpose, for how long, whether we transfer your data to anyone (e.g. to our accountant), or whether we transfer your data to a controller or processor established in a country

outside the European Union. Transparency includes your right to be informed about all of this and our obligation to bring this information to your attention.

It is important to note that there are limits to our obligation to provide information. This obligation does not mean that we must personally contact each and every individual whose data we process, but the fact of the processing must always be brought to your attention. The manner of providing information is regulated by several pieces of legislation and guidance, and in some cases – for companies with a website, including us – it is sufficient to provide information in a notice published on the website. In some stricter cases, however, we are required to inform the data subject about a specific change in processing by e-mail.

The GDPR also provides that if we do not obtain your personal data from you directly but from another person, we must inform you of this at the earliest possible opportunity, at the time of the first contact with you, but at the latest within one month.

2.2 Necessity and proportionality

Fundamental rights may only be restricted where necessary and proportionate. Necessity means that the data processing is strictly required in order to achieve the purpose of processing. Proportionality sets the limits of this necessity by requiring that any restriction of fundamental rights and freedoms arising from processing must also be proportionate to the objective pursued.

The Fundamental Law of Hungary provides that a fundamental right may be restricted in order to ensure another fundamental right or to protect a constitutional value, to the extent absolutely necessary, proportionately to the objective pursued, and with due respect for the essential content of the fundamental right. When processing your personal data, we fully comply with the principle of necessity and proportionality.

2.3 Purpose limitation

We collect personal data only for specified, explicit and legitimate purposes and do not process them in a manner incompatible with those purposes. This means that we always determine the purpose of processing before starting to process data and process the data solely for that purpose. This purpose is never contrary to the law. It is important to note, however, that we may process a particular item of your data for more than one purpose, but in such cases we regulate the processing separately for each purpose. For example, we may process your name for the purpose of preparing an offer, later for performance once you become our customer, and after the purchase for invoicing purposes. In these three cases, the purposes of processing are clearly different, as in the case of a request for quotation, processing is based on the preparation of the contract, after the order it is based on the performance of the contract, and after issuing the invoice we process your data based on a statutory obligation.

Processing may also take place for several purposes in parallel. For example, after performance of the contract, we may retain documents containing your data for the purpose of asserting our legitimate interests, such as evidence in a future dispute, while we process the same data on the invoice on the basis of a statutory obligation to retain accounting documents.

If the purposes of processing change, you must always be informed accordingly.

According to the GDPR, further processing for the purposes of archiving in the public interest, scientific or historical research or statistical purposes is not considered to be incompatible with the original purpose.

2.4 Data minimisation

We process personal data in a manner that is adequate, relevant and limited to what is necessary in relation to the purposes. We do not process data that are not necessary for achieving the purpose.

2.5 Accuracy

We keep personal data accurate and up to date to the best of our knowledge. Where possible, we take all reasonable measures to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay. However, unrealistic expectations cannot be imposed on a controller. For example, we cannot call everyone every day to check whether their name is still the same. If, however, you become aware that your personal data have changed or have reached us incorrectly, and rectification is not contrary to the purpose of processing, such data must be corrected, and you must notify us of the change.

Our obligation is to strive to comply with the requirement of accuracy, but, naturally, if you become aware that we are processing inaccurate data relating to you, you are also obliged to inform us.

2.6 Storage limitation

We store personal data in a form which permits your identification only for as long as is necessary for the purposes for which the personal data are processed. After this period, we erase the data. Our IT system is designed so that electronically stored data are erased upon the expiry of the applicable retention period. The exact retention periods and the rules for the disposal of data are set out in our internal data processing policy, and we always act in accordance with those rules. We do not retain data unnecessarily.

We only store your personal data for a longer period than the above if processing is carried out in accordance with the GDPR for the purposes of archiving in the public interest, scientific or historical research or statistical purposes, subject to the implementation of appropriate technical and organisational measures as required by the GDPR in order to protect your rights and freedoms.

2.7 Integrity and confidentiality

We process your personal data in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical and organisational measures. Our data storage has been designed so that even within the company, unauthorised persons cannot access the data. For example, a specialist colleague who is not involved in the online ordering process does not use webshop order data; the internal access rights of our organisation are configured in such a way that this person cannot see such data.

2.8 Accountability

The Controller is responsible for, and must be able to demonstrate, compliance with the data protection rules. How is this done? Who holds a Controller to account? In Hungary, this is the National Authority for Data Protection and Freedom of Information (NAIH).

Upon a notification (and in some cases ex officio), NAIH examines whether the data processing activities of a given company are lawful and comply with all legal requirements. In such a procedure, the Controller must be able to demonstrate and prove that it carries out its data processing in compliance with the relevant legislation. A key tool in this respect is the existence of an appropriate data protection policy, in which data processing must be regulated in a lawful manner. It is equally

important that if we have a good, i.e. legally compliant, policy, we actually carry out our processing activities in accordance with it. A good policy alone is not sufficient.

The Controller has developed a comprehensive data processing and data security policy for its entire processing operation and carries out its data processing in line with this policy.

3. Lawfulness of Processing

When designing our data processing activities, we always ensure that the processing of personal data is lawful in accordance with the principle of lawfulness. We carry out our data processing on the following legal bases, taking into account the specific detailed rules.

3.1 Consent of the data subject

You have given your consent to the processing of your personal data for one or more specific purposes. It is important that consent is given freely and that you provide your consent by way of a clear, affirmative act in every case.

3.2 Performance of a contract

Processing is necessary for the performance of a contract to which you are a party, or in order to take steps at your request prior to entering into a contract.

3.3 Compliance with a legal obligation

Processing is necessary for compliance with a legal obligation to which we are subject. We only process data on the legal basis of a legal obligation where we are expressly required to do so by law. We do not rely on this legal basis in cases where the relevant law merely provides for data processing in conditional or optional terms.

3.4 Protection of vital interests

Processing is necessary in order to protect your vital interests or those of another natural person. A key consideration in choosing this legal basis is that processing based on vital interests is of a temporary nature and may only last as long as the vital interest exists. We lay down separate rules for the processing of the data once the vital interest has ceased to exist.

3.5 Public interest or exercise of official authority

In such cases, processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us. We are not an authority and we do not carry out processing in the public interest; therefore, we do not currently process data on this legal basis.

3.6 Legitimate interests

Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require the protection of personal data, in particular where the data subject is a child. We frequently rely on this legal basis in the course of our processing activities.

Where processing is based on legitimate interests, we always carry out a legitimate interest balancing test in which we assess the necessity and proportionality of the impact and any restriction on your fundamental rights and freedoms.

4. Data Security

The Controller is committed to protecting personal data against loss, unlawful use, unlawful transmission, alteration, inaccessibility or destruction, and takes all necessary measures to preserve the confidentiality of personal data, including the application of appropriate technical and organisational measures.

Our organisational measures include, in particular, controlling physical access to our premises, training our employees and keeping paper-based files in locked, properly secured rooms. Our technical measures include the use of encryption and password protection in connection with access to our systems, as well as the use of antivirus software.

As part of the process by which you provide us with your personal data, these data may also be transmitted over the internet. Although we take all necessary steps to protect the personal data you provide to us, transmission of data over the internet cannot be regarded as completely secure. Accordingly, you must acknowledge and accept that we cannot assume full responsibility for the security of data transmitted through our website and that such transmission is at your own risk. Once your personal data have reached our systems, however, we apply strict procedures and measures to ensure security and to prevent unauthorised access.

In cases where we have provided you with a password (or where you have chosen one), you are responsible for keeping this password confidential. We kindly ask you not to disclose this password to anyone.

Our websites and social media pages may from time to time contain links to websites operated by third parties, including group companies and partner networks. Any data processing carried out on such external websites does not form part of our processing activities.

5. Parties involved in data processing and their roles

In the course of data processing activities, the Controller independently determines the purposes and means of processing personal data and is responsible for the lawfulness of processing and for compliance with the applicable European Union and Hungarian legislation. The Controller decides for what purposes, on what legal basis, which data and for how long are processed, and defines the organisational and technical framework of processing.

The Controller may engage processors to perform certain technical, administrative or IT tasks. A processor is a natural or legal person who processes personal data on behalf of the Controller and exclusively in accordance with the Controller's instructions. The processor does not independently determine the purposes and means of the processing; it processes the data solely within the framework defined by the Controller and must apply appropriate technical and organisational measures to ensure the security of personal data. The Controller concludes contracts with processors that comply with the relevant legal requirements.

Partners involved in the performance of travel and event organisation services – in particular airlines, accommodation providers, insurers and other service providers – process the personal data transferred to them as independent controllers. These service providers determine their own processing purposes and means autonomously, and their processing is governed by their own privacy notices and internal

policies. The Controller is not responsible for the data processing activities of these independent controllers.

List of key partners

Name	Role	Contact details
SKDNZ Ingatlanhasznosító Kft.	Controller	1123 Budapest, Alkotás út 55–61.
Unione Management Kft.	Controller (data recipient) – marketing activities, newsletter sending	1123 Budapest, Alkotás út 55–61.
TPLC Zrt.	Processor – maintenance and operation of IT systems	1033 Budapest, Szentendrei út 89–95.
Unione Management Kft.	Processor – accounting and invoicing	1123 Budapest, Alkotás út 55–61.
Raiffeisen Bank Zrt.	Account-holding bank	1133 Budapest, Váci út 116–118.
OTP Bank Nyrt.	Card payment service provider	1051 Budapest, Nádor u. 16.
Tableversum – PG Info Kft.	Operator of the table reservation system	9141 Ikrény, Sport u. 22.
Unione Hotel Management Kft.	Processing and management of job applications – HR activities (excluding payroll accounting)	1123 Budapest, Alkotás út 55–61.

Within certain contractual relationships – in particular in the context of travel organisation, travel agency or event organisation services – the Controller may act not as an independent controller but as a processor. In such cases, the Controller processes personal data for the purposes and within the framework defined by one of its contractual partners (its client), and on the basis of that partner's instructions. In the course of such processing, the Controller does not independently determine the purposes and means of processing; it processes the data exclusively in accordance with the documented instructions of the client-controller and transfers them to third parties only on the basis of the client's instructions or a statutory obligation.

Such processing activities are governed by the contract concluded between the parties and by the data processing agreement drawn up in accordance with Article 28 of the GDPR. The rights of data subjects

are primarily exercised vis-à-vis the client-controller; however, in its capacity as processor, the Controller cooperates with the client-controller in order to fulfil data subject requests.

6. Purposes and legal bases of individual processing operations

Purpose of processing	**Legal basis (GDPR + full title of Hungarian law)**	**Categories of personal data processed**	**Retention period**	**Processing / data transfers**
1. Preparation of contracts (requests for quotation, information requests, contact)	GDPR Article 6(1)(b) – steps prior to entering into a contract; Act V of 2013 on the Civil Code	Name, e-mail address, telephone number, corporate contact details, content of the enquiry	In the absence of a contract, max. 12 months	E-mail and correspondence system
2. Conclusion and performance of contracts	GDPR Article 6(1)(b) – performance of a contract; Act V of 2013 on the Civil Code; Government Decree No. 472/2017 (XII. 28.) on travel services	Name, date of birth, address, ID document data, contact details, payment data	5 years after termination of the contract	Accountant
3. Fulfilment of accounting and tax obligations (invoicing, bookkeeping)	GDPR Article 6(1)(c) – compliance with a legal obligation; Act C of 2000 on Accounting (Sections 166–169); Act CXXVII of 2007 on Value Added Tax; Act CL of 2017 on the Rules of Taxation	Invoicing name, address, tax number, performance-related data	8 years	Accountant; tax authority; account-holding bank
4. Handling of complaints	GDPR Article 6(1)(c) – compliance with a legal obligation;	Name, contact details, content of the complaint	5 years	Data transfer to authorities; data transfer to legal representative

Purpose of processing	Legal basis (GDPR + full title of Hungarian law)	Categories of personal data processed	Retention period	Processing / data transfers
	Act C of 2000 on Accounting, Section 17/A(7); Act CLV of 1997 on Consumer Protection; Act V of 2013 on the Civil Code			
5. Lodging and defence of legal claims	GDPR Article 6(1)(f) – legitimate interest in the enforcement and defence of legal claims	Data related to the case	Until expiry of the limitation period	Courts; legal representative
6. Technical operation of the website	GDPR Article 6(1)(f) – legitimate interest in the operation and security of the website	IP address, log data	90 days	Hosting provider
7. Use of cookies – necessary cookies	GDPR Article 6(1)(f) – legitimate interest	Technical cookie data	Until the end of the session	IT service provider
8. Use of cookies – statistical and marketing cookies	GDPR Article 6(1)(a) – consent	Cookie identifiers, browsing data	Until withdrawal of consent	External analytics provider (Google Analytics)
9. Newsletters and direct marketing communication	GDPR Article 6(1)(a) – consent	Name, e-mail address	Until withdrawal of consent	Data transfer to Unione Management Zrt.; newsletter service provider

Purpose of processing	Legal basis (GDPR + full title of Hungarian law)	Categories of personal data processed	Retention period	Processing / data transfers
10. Processing of job applications	GDPR Article 6(1)(b) – steps prior to entering into an employment contract	Name, contact details, data contained in the CV	Max. 6 months	Where submitted by e-mail: IT service provider; processor – Unione Hotel Management Kft.
11. Contact with prospects, business partners and agents	GDPR Article 6(1)(b) – steps prior to entering into a contract; performance of a contract	Name, position, contact details	For the duration of the business relationship	IT service provider

7. Provisions on data transfers and use of processors

The Controller handles personal data confidentially and transfers them to third parties only where necessary for compliance with a legal obligation, for the performance of a contract, on the basis of the data subject's consent, or where another legal basis under Article 6 of the GDPR exists. Any transfer of data is always carried out in line with the principles of purpose limitation and data minimisation and is restricted to the scope of data that is necessary.

To comply with its statutory obligations, the Controller may transfer personal data in particular to the National Tax and Customs Administration for the purpose of fulfilling tax and accounting obligations, and to the National Tourism Data Supply Centre for the purpose of performing mandatory data reporting obligations related to catering activities. The legal basis for such transfers is Article 6(1)(c) of the GDPR (compliance with a legal obligation).

For the performance of marketing and sales activities and for organising the sending of newsletters, the Controller transfers personal data to its parent company, Unione Management Kft. The purpose of the transfer is the coordinated, central management of marketing and sales activities of the hotels and catering units owned by the parent company. The legal basis for the transfer is the data subject's consent under Article 6(1)(a) of the GDPR in the case of newsletters, and the legitimate interest under Article 6(1)(f) of the GDPR in the case of other marketing activities, namely the interest in ensuring group-wide, unified marketing activities. The parent company processes the transferred data in accordance with the applicable data protection legislation.

The Controller operates as a member of the Unione Group. Recruitment and selection processes within the group are organised and coordinated by Unione Hotel Management Kft. The personal data provided in application materials may be made available by Unione Hotel Management Kft. to other group companies in order to offer the applicant job opportunities at another group company and to organise interviews. The group company at which the establishment of an employment relationship is envisaged acts as an independent controller in relation to the application data. The legal basis for this data transfer

is the data subject's consent as defined in Article 6(1)(a) of the GDPR, which is given by submitting the application or by a separate declaration.

To ensure its economic operation and the provision of services, the Controller may use further processors, in particular accounting service providers, IT operators, cash register and catering software providers, banking and electronic payment service providers, and – where relevant – operators of online ordering systems. Processors act on the basis of a contract concluded with the Controller, solely in accordance with the Controller's documented instructions, and implement appropriate technical and organisational measures to protect personal data.

The Controller may transfer personal data to courts, authorities or other public bodies where this is required by law or where a lawful request is made. The legal basis for such transfers is Article 6(1)(c) of the GDPR.

As a general rule, the Controller does not transfer personal data to countries outside the European Union. Where the use of IT or cloud services makes it necessary to transfer data to a third country, such transfer will only take place subject to the application of appropriate safeguards as set out in Chapter V of the GDPR.

8. Your rights

If you wish to exercise any of your rights described below (such as requesting the transfer, erasure or rectification of your data), please contact us using any of our contact details or by filling in the form available at the end of this section.

1. **Right to information**
   We must provide you with information that is appropriately detailed, in a suitable language, written in clear and simple terms and easy to find, covering the essential aspects of processing (what data is used, for what purpose, how, and for how long, etc.), and the GDPR specifies in detail the required scope of information. Where possible, information must be provided before personal data are collected. If this is not possible – for example where data are obtained from a third party – information is provided at the first possible opportunity.

2. **Right of access**
   You may request information as to whether we process personal data relating to you and, if so, which of your data we process and under what conditions. The conditions that can be requested are described in more detail in the section on the right to information above.

3. **Right to rectification**
   You may notify us if the data we process are inaccurate and may request that we replace them with accurate data. If you become aware that your data are inaccurate or incorrect, please inform us as soon as possible and we will rectify them.

4. **Right to erasure ('right to be forgotten')**
   You may request, in the cases and under the conditions laid down by law, that we erase your data from our databases. This applies for example where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, or where you withdraw your consent and there is no other legal basis for processing.

Unfortunately, there are situations in which we must refuse your request for erasure. One such case is where we are required by law to retain data (for example, data used for invoicing must, as a general

rule, be kept for 8 years in accordance with the relevant legislation). We may also refuse erasure on the basis of legitimate interests – for example for the purpose of evidence in later proceedings – within the limitation period. Beyond these examples, there are numerous other cases where processing may lawfully continue despite an objection. As is generally the case in data protection, each case is individual and must be assessed on its own merits when determining whether refusal of erasure is lawful.

5. **Right to restriction of processing**
   You may request, in the cases and under the conditions laid down by law, that we restrict the processing of your data for a (possibly legally defined) period. As a general rule, data subject to restriction may only be stored, and no other operations may be carried out on them, subject to the exceptions laid down by law. When the restriction is lifted, we will notify you.

You may request restriction in the following cases:

- You contest the accuracy of the personal data; in this case the restriction applies for a period enabling us to verify the accuracy of the personal data.
- The processing is unlawful but you oppose the erasure of the data and request the restriction of their use instead.
- We no longer need the personal data for the purposes of the processing, but you require them for the establishment, exercise or defence of legal claims.
- You have objected to processing; in this case the restriction applies for the period during which it is verified whether our legitimate grounds override yours.

6. **Right to data portability**
   You may request to receive the personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format (such as .doc, .pdf, etc.) and you have the right to transmit those data to another controller without hindrance from us. The GDPR thus facilitates the possibility for you to move your personal data from one controller to another. This right is only available where processing is carried out by automated means.

7. **Right to object and rights related to automated decision-making**
   You have the right, in certain cases, to object to the processing of your personal data. In the event of an objection, we may no longer process the data concerned, unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defence of legal claims. You may also, in certain circumstances, request not to be subject to a decision based solely on automated processing. This presupposes, among other things, that such automated decision-making is not necessary for entering into or performing a contract between you and us and that we are not legally required to use automated decision-making in the given case.

9. Remedies

Please contact us first; we will do our utmost to resolve your problem. If this is not possible or you do not wish to contact us, you may lodge a complaint with the data protection authority or bring an action before the courts.

Contact details of the Hungarian data protection supervisory authority:

National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság)

Postal address: 1363 Budapest, Pf. 9.

Address: 1055 Budapest, Falk Miksa utca 9–11.

Telephone: +36 (1) 391 1400

E-mail: ugyfelszolgalat@naih.hu

Website: https://naih.hu

Right to bring proceedings before the courts:

If your rights as a data subject are infringed, you may also bring an action against the Controller before a court. You may choose to bring the action before the court with jurisdiction over your place of residence or habitual residence.

10. Validity of this Policy

This Policy is valid from 1 January 2026 until withdrawn.