GDPR – PRIVACY POLICY

1. Introduction

Dél-Alföld Consulting Kft. (registered office: 6750 Algyő, Külterület Hrsz.: 01767/89., tax number: 13730549-2-06, company registration number: 06-09-015120) (hereinafter: Service Provider, Data Controller) hereby subjects itself to the following policy:

In accordance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the following information is provided.

This Privacy Notice regulates the data processing activities associated with the operation of the website https://larougehotel.com/ and the La Rouge Boutique Hotel.

The Privacy Notice is available at the following webpage:
https://larougehotel.com/adatvedelem

Amendments to this Notice shall take effect upon publication at the above URL.

1.1. The Data Controller and Contact Information

- **Name:** Dél-Alföld Consulting Kft.
- **Registered Office:** 6750 Algyő, Külterület Hrsz.: 01767/89.
- **Place of Business:** 1052 Budapest, Semmelweis utca 25.
- **E-mail:** info@larougehotel.com
- **Phone:** +36 70 479 91 04
- **Website:** https://larougehotel.com/

2. Definitions

- **2.1. "personal data":** means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification 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;
- **2.2. "processing":** means 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **2.3. "controller":** means the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- **2.4. "processor":** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **2.5. "recipient":** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- **2.6. "consent" of the data subject:** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **2.7. "personal data breach":** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3. Principles Relating to Processing of Personal Data

Personal data shall be:

- **a)** processed lawfully, fairly and in a transparent manner in relation to the data subject (**"lawfulness, fairness and transparency"**);
- **b)** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**"purpose limitation"**);
- **c)** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**"data minimisation"**);
- **d)** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**"accuracy"**);
- **e)** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**"storage limitation"**);
- **f)** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**"integrity and confidentiality"**).

The controller shall be responsible for, and be able to demonstrate compliance with the above (**"accountability"**).

The Data Controller declares that its data processing operations are conducted in accordance with the principles set forth in this section.

Legal Basis for Data Processing within this Policy:

1. Article 6(1)(b) and (c) of the GDPR.
2. Section 13/A (3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (hereinafter: E-Commerce Act):

   The service provider may, for the purpose of providing the service, process personal data that are technically indispensable for the provision of the service. In the event of other conditions being equal, the service provider must choose and in all cases operate the means used in the provision of information society services in such a manner that personal data are processed only if it is strictly necessary for the provision of the service and the fulfillment of other objectives specified in this Act, but even in this case, only to the extent and for the duration necessary.

3. For the purpose of issuing invoices complying with accounting legislation: Article 6(1)(c) of the GDPR.
4. For the enforcement of claims arising from contracts: 5 years pursuant to Section 6:21 of Act V of 2013 on the Civil Code.

   Section 6:22

   $$Limitation Period$$
   (1) Unless otherwise provided by this Act, claims shall lapse after five years.

   (2) The limitation period begins when the claim becomes due.

   (3) Any agreement to alter the limitation period must be concluded in writing.

   (4) An agreement excluding the limitation period shall be null and void.

Please be informed that:

- Data processing in the event of requests for quotes and bookings is based on the performance of a contract or is necessary to take steps at your request prior to entering into a contract.
- You are obliged to provide personal data so that we are able to fulfill the booking.
- Failure to provide data will result in the consequence that we cannot process your booking or request for a quote.

4. Categories of Data Processing and Data Processors

Room Bookings, Requests for Quotes, Event Proposals

- **Scope of Processed Data:** Name, e-mail address, telephone number, billing name and address, reservation details, event-related details, IP address, technical data, food allergy or special dietary information (if voluntarily provided by the data subject).

- **Purpose of Processing:** Provision of quotes, management of accommodation bookings, event and wedding planning, communication, performance of the contract, invoicing, and compliance with legal obligations.
- **Duration of Processing:**
    - In the case of requests for quotes: up to 2 years.
    - In the case of contracts: until the end of the civil law limitation period.
    - In the case of accounting source documents: 8 years.

The Service Provider utilizes the SabeeApp hotel management software to handle reservations, offers, and guest data.

- **Data Processor:** thePass Kft. / SabeeApp
  Address: 1053 Budapest, Reáltanoda utca 5. 4th floor

Contacting the Hotel

The Service Provider processes the data of individuals who contact the hotel via the website, e-mail, telephone, or social media platforms for the purpose of communication and responding to inquiries.

- **Processed Data:** Name, e-mail address, telephone number, content of the message.
- **Duration of Processing:** The Service Provider retains this data for a maximum of 2 years.

Customer Relations

The Service Provider processes data handled during customer relations for the purposes of contract performance, provision of quotes, and business communication.

- **Processed Data:** Name, e-mail address, telephone number, contact details.
- **Duration of Processing:** Up to 2 years, or in the event of a legal claim, until the end of the limitation period.

Table Reservations and Restaurant Consumption

- **Processed Data:** Name, telephone number, e-mail address, consumption details, billing data, signed consumption receipt or charge slip.
- **Purpose of Processing:** Managing table reservations, recording consumption, invoicing, accounting, and enforcement of legal claims.

The Service Provider uses the Fruitsys hospitality system to manage hospitality consumption and orders.

- **Data Processor Details:** Fruitsys Kft.
  Registered Office: 1073 Budapest, Akácfa utca 54. ground floor, Unit 2 (szint Ü2. ajtó)
  Website: https://fruitsys.hu/
  E-mail: info@fruitsys.hu
- **Retention Period:** Signed consumption receipts and charge slips are retained by the Service Provider for 1 year. For accounting documents, the retention period is 8 years.

Complaint Handling

The Service Provider processes data related to the handling of consumer complaints in accordance with the relevant consumer protection legislation.

- **Retention Period:** Documents related to complaint handling are retained by the Service Provider for 5 years.

Accounting and Bookkeeping Data Processing

- **Processed Data:** Billing name, billing address, tax number, invoice details, payment details, service details.
- **Purpose of Processing:** Invoicing, bookkeeping, filing, and fulfillment of accounting obligations.

The Service Provider utilizes the Libra Soft accounting and filing software during bookkeeping and archiving tasks.

- **Data Processor Details:** Libra Szoftver Zrt.
  Registered Office: 1114 Budapest, Bocskai út 77-79.
  Website: https://www.libra.hu/
  E-mail: info@libra.hu
- **Retention Period:** 8 years pursuant to the Accounting Act.

Data Processing Related to the VIZA System

In the course of providing accommodation services, the Service Provider is obliged to fulfill statutory obligations regarding the recording and transmission of guest data.

- **Processed Data:** Name, birth name, place and date of birth, nationality, mother's maiden name, identification document data, residential address, dates of arrival and departure.
- **Purpose of Processing:** Fulfillment of legal obligations, data transmission to the VIZA system, and provision of accommodation services.
- **Duration of Processing:** For the duration specified in the relevant legislation.

Website and E-mail System

The Service Provider engages an external data processor for the operation, technical maintenance, hosting, and e-mail services of the website.

- **Data Processor Details:** INTROWEB Szolgáltató és Kereskedelmi Korlátolt Felelősségű Társaság
  Registered Office: 6724 Szeged, Gelei József utca 5. I. floor 3.
  E-mail: info@introweb.hu
  Website: https://www.introweb.hu
  Phone: +36 20 414 2574
- **Nature of Data Processing:** The data processor performs the technical operation of the website, provision of e-mail services, web hosting, system administration, technical support tasks, and the maintenance of web systems. In the course of operation, the data processor may have technical access to personal data handled

on the website, in electronic correspondence, or in connected systems; however, it may process them exclusively based on the instructions of the Service Provider.

Cookies

The website uses cookies to ensure its operation, as well as for statistical analysis and marketing purposes.

- **Cookie Types:** Session cookies, statistical cookies, marketing cookies, functional cookies.
- Visitors are informed about the use of cookies via a cookie banner.

Data Processing Related to Job Applications

The Service Provider processes CVs and related documents submitted during job applications exclusively for recruitment purposes.

- **Processed Data:** Name, contact details, information contained in the CV, professional experience, qualifications, and photograph (if provided by the applicant).
- **Duration of Processing:** Until the end of the selection process, up to a maximum of 1 year.

NTAK Data Reporting

In order to fulfill its legal obligations, the Service Provider reports data to the National Tourism Data Supply Centre (NTAK). The catering and hospitality data transmitted to NTAK are statistical in nature and do not contain personal data.

5. Rights of the Data Subjects

5.1. Right of Access

You have the right to obtain from the controller confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and the information listed in the Regulation.

5.2. Right to Rectification

You have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

5.3. Right to Erasure ("Right to be Forgotten")

You have the right to obtain from the controller the erasure of personal data concerning you without undue delay, and the controller shall have the obligation to erase personal data without undue delay under specific conditions.

5.4. Right to the Restriction of Processing

You have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by you, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims;
- you have objected to processing; in this case, the restriction applies for a period pending the verification whether the legitimate grounds of the controller override those of yours.

5.5. Right to Data Portability

You have the right to receive the personal data concerning you, which you have provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (...)

5.6. Right to Object

Where personal data are processed based on legitimate interest or the exercise of official authority as legal bases, you have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you (...), including profiling based on those provisions.

5.7. Objection in the Case of Direct Marketing

Where personal data are processed for direct marketing purposes, you have the right to object at any time to processing of personal data concerning you for such marketing, which includes profiling to the extent that it is related to such direct marketing. If you object to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

5.8. Automated Individual Decision-Making, Including Profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

The previous paragraph shall not apply if the decision:

- is necessary for entering into, or performance of, a contract between you and a data controller;
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests; or
- is based on your explicit consent.

6. Time Limit for Action

The controller shall provide information on action taken on a request to you without undue delay and in any event within 1 month of receipt of the request.

Where necessary, this period may be extended by 2 further months. The controller shall inform you of any such extension within 1 month of receipt of the request, together with the reasons for the delay.

If the controller does not take action on your request, the controller shall inform you 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.

7. Data Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:

- **a)** the pseudonymisation and encryption of personal data;
- **b)** the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- **c)** the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- **d)** a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- **e)** processed data must be stored in such a manner that unauthorized persons cannot access them. For paper-based data carriers, this is achieved by establishing physical storage and archiving protocols; for electronically processed data, by applying a centralized access management system;
- **f)** the IT method for storing data must be chosen so that its erasure can be executed upon the expiry of the data retention period—taking into account potentially differing erasure deadlines—or when it becomes necessary for other reasons. Erasure must be irreversible;
- **g)** paper-based data carriers must be stripped of personal data using a paper shredder or by engaging an external organization specializing in document destruction. In the case of electronic data carriers, physical destruction must be ensured in accordance with the rules on discarding electronic media, or, as necessary, by secure and irreversible deletion of data beforehand;
- **h)** The controller implements the following specific data security measures:
    - **a. Measures applied by the Service Provider to ensure the security of personal data processed on paper (physical protection):**
        - i. Documents must be placed in a secure, well-lockable, dry room.
        - ii. The building and premises of the Service Provider are equipped with fire protection and property security systems.

        - iii. Personal data may only be accessed by authorized persons; third parties shall not have access to them.
        - iv. The data processing employee of the Service Provider may only leave the room where data processing takes place during their work by locking away the data carriers entrusted to them or by locking the room in question.
        - v. If personal data processed on paper are digitalized, the rules governing digitally stored documents shall apply.
    - **b. IT Protection:**
        - i. Computers and mobile devices (other data media) used during data processing constitute the property of the Service Provider.
        - ii. Data stored on computers can only be accessed with a username and password.
        - iii. The central server machine can only be accessed with appropriate authorization and exclusively by designated persons.
        - iv. To ensure the security of digitally stored data, the Service Provider utilizes data backups and archiving.
        - v. The computer system containing personal data used by the Service Provider is equipped with anti-virus protection.
        - vi. Encrypted channel (SSL).
        - vii. The Data Controller ensures:
            2. the ongoing confidentiality, integrity, availability, and resilience of the systems and services used to process personal data;
            3. the ability to restore access to and availability of personal data in a timely manner in the event of a physical or technical incident.

8. Informing the Data Subject about a Personal Data Breach

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the name and contact details of the data protection officer or other contact point where more information can be obtained; describe the likely consequences of the personal data breach; describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication to the data subject shall not be required if any of the following conditions are met:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the

personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

9. Reporting a Personal Data Breach to the Authority

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

10. Mandatory Review in the Case of Compulsory Data Processing

If the duration of compulsory data processing or the periodic review of its necessity is not defined by law, local municipal decree, or a binding legal act of the European Union, the controller shall review at least every three years from the commencement of data processing whether the processing of personal data handled by it, or by a data processor acting on its behalf or under its instructions, is necessary for the realization of the purpose of data processing.

The circumstances and results of this review shall be documented by the controller, and this documentation shall be retained for ten years following the performance of the review and made available to the National Authority for Data Protection and Freedom of Information (hereinafter: Authority) upon the Authority's request.

11. Right to Lodge a Complaint

Complaints against potential infringements by the data controller may be lodged with the National Authority for Data Protection and Freedom of Information:

National Authority for Data Protection and Freedom of Information (NAIH)

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Mailing Address: 1530 Budapest, Postafiók: 5.

Telephone: +36 1 391 1400

E-mail: ugyfelszolgalat@naih.hu

12. Closing Provisions

This Notice has been prepared with due regard to the GDPR, the Info Act (Act CXII of 2011), the Accounting Act, legislation on electronic commerce services, as well as current Hungarian legislation governing data processing in the tourism and hospitality industries.

The Service Provider reserves the right to modify this Notice.