PRIVACY NOTICE
Concerning the Rights of the Data Subject Regarding the Processing of Personal Data

TABLE OF CONTENTS

INTRODUCTION

The European Parliament and Council's Regulation (EU) 2016/679 (hereinafter referred to as the Regulation), on the protection of natural persons concerning the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC, mandates that the Data Controller take appropriate measures to ensure that all information provided to the data subject concerning the processing of personal data is concise, transparent, understandable, and easily accessible, clearly and intelligibly communicated. Furthermore, the Data Controller must facilitate the exercise of the data subject's rights.

The obligation to inform the data subject in advance is also required by Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.

This notice fulfills our statutory obligations by providing this information below.

The notice must be published on the company's website or sent to the data subject upon request.

CHAPTER I
IDENTIFICATION OF THE DATA CONTROLLER

The issuer of this notice, and the Data Controller:
Company Name: Homoky Hotels Tiliana Hotel Kft.
Headquarters: 1021 Budapest, Hárshegyi út 1-3
Company Registration Number: 01-09-296382
Tax Number: 25921580-2-41
Representative: László Endre Homoky
Phone Number: +36 1 391 0027
Email Address: info@hoteltiliana.hu
Website: www.tiliana.hu
(hereinafter referred to as the Company)

CHAPTER II
IDENTIFICATION OF DATA PROCESSORS

Data Processor: Any natural or legal person, public authority, agency, or other body that processes personal data on behalf of the Data Controller. (Regulation Article 4, Section 8)

The involvement of a data processor does not require the prior consent of the data subject, but notification is necessary. Accordingly, we provide the following information:

1. Our Company's IT Service Provider

Our Company engages a data processor to maintain and manage its website, who provides IT services (hosting services). As part of this arrangement, and for the duration of our contract with this provider, they process personal data provided on the website. The data processing activity carried out by this provider involves the storage of personal data on the server.

The details of this data processor are as follows:

Company Name: Dobom Alkotó Tér Kft
Headquarters: 8764 Zalaszentmárton, Kossuth u. 47
Company Registration Number:
Tax Number: 24661544-1-20
Representative: Márton Dobay
Phone Number: +36 30 276 2485
Email Address: info@dobom.hu
Website: www.tiliana.hu

2. Our Company's Accounting Service Provider

Our Company engages an external service provider through an accounting services contract to fulfill its tax and accounting obligations. This provider processes personal data of individuals who have contractual or payee relationships with our Company, solely for the purpose of fulfilling our tax and accounting responsibilities.

The details of this data processor are as follows:

Company Name: BÁNFFY-HÁZ Bt.
Headquarters: 6000 Kecskemét, Árok utca 39 FSZ/5
Tax Number: 20175760203
Representative: Mária Tóth
Phone Number: +36 70 60 43329

3. Postal Services, Delivery, Parcel Shipping

These data processors receive from our Company the personal data necessary for the delivery of ordered products (name, address, phone number of the data subject) and use this information to complete the delivery.

The service providers are as follows:

Hungarian Post (Magyar Posta)

Courier Service

Company Name:
Headquarters:
Company Registration Number:
Tax Number:
Representative:
Phone Number:

4. Security Service Provider

This data processor, contracted by our Company for the duration of our agreement, conducts workplace video surveillance and access control, along with the associated data processing activities. The service provider is as follows:
Company Name:
Headquarters:

Company Registration Number:
Tax Number:
Representative:
Phone Number:

CHAPTER III

DATA PROCESSING RELATED TO EMPLOYMENT

1. Munkaügyi, személyzeti nyilvántartás

Employment and Personnel Records

(1) Only data necessary for establishing, maintaining, or terminating the employment relationship, or for providing social and welfare benefits, may be requested and recorded from employees. Additionally, only job-related medical suitability examinations required for these purposes may be conducted, ensuring the protection of the employee's personal rights.

(2) Based on the legal grounds of the Company's legitimate interest as an employer (Regulation Article 6, Section 1(f)), the following personal data of the employee may be processed for the purpose of establishing, performing, or terminating the employment relationship:

1. Name
2. Birth name
3. Date of birth
4. Mother's name
5. Address
6. Nationality
7. Tax identification number
8. Social security number (TAJ number)
9. Pensioner identification number (if applicable for retired employees)
10. Phone number
11. Email address
12. Personal ID number
13. Address verification document number
14. Bank account number
15. Online identifier (if applicable)
16. Start and end dates of employment
17. Job title
18. Copy of documents verifying educational qualifications and professional certifications
19. Photograph
20. Curriculum vitae (CV)
21. Salary amount, payroll, and other benefit information

22. Deductions from salary due to enforceable court order, law, or written consent, and the basis for such deductions
23. Performance evaluations
24. Method and reasons for termination of employment
25. Certificate of good conduct (depending on the job position)
26. Summary of job-related medical suitability examinations
27. For private pension fund and voluntary mutual insurance fund membership, the name of the fund, identification number, and employee membership number
28. For foreign employees, passport number and name and number of the document verifying employment eligibility
29.
30. Data recorded in accident reports related to accidents involving the employee
31. Data necessary for utilizing welfare services or commercial accommodation
32. Data recorded by the Company's security and surveillance systems, including cameras, access control, and location tracking systems

(3) Data concerning health and union membership may only be processed by the employer for the purpose of fulfilling rights or obligations specified in the Labor Code.

(4) Recipients of Personal Data: The recipients of the personal data include the employer's management, those exercising employer rights, and employees and data processors handling HR tasks within the Company.

(5) Only the personal data of senior employees may be forwarded to the Company's owners.

(6) Data Retention Period: Personal data will be retained for three years following the termination of employment.

(7) Notification Requirement: Before commencing data processing, the data subject must be informed that the processing is based on the Labor Code and on the legitimate interests of the employer.

2. Data Processing Related to Suitability Examinations

(1) Only suitability examinations required by employment regulations, or necessary for exercising rights or fulfilling obligations specified in such regulations, may be applied to the employee. Prior to the examination, employees must be informed in detail about the purpose of the examination, including the specific skills or abilities being assessed, and the methods or tools used in the examination. If the examination is mandated by law, employees must also be informed of the title and specific citation of the law.

(2) Suitability or preparedness tests may be administered by the employer both prior to the establishment of employment and during the employment relationship.

(3) Psychological or personality tests, intended to improve the organization and efficiency of work processes, may be conducted with larger employee groups only if the data revealed through analysis cannot be associated with specific employees, ensuring data is processed anonymously.

(4) Scope of Personal Data Processed: The fact of job suitability and the conditions necessary for it.

(5) Legal Basis for Data Processing: The legitimate interest of the employer.

(6) Purpose of Data Processing: To establish and maintain the employment relationship and to determine job suitability.

(7) Recipients of Personal Data or Categories of Recipients: The results of the examination can only be accessed by the examined employee and the specialist conducting the examination. The employer is only informed whether the employee is suitable for the job and what conditions, if any, must be ensured for suitability. However, the employer does not have access to the details or full documentation of the examination.

(8) Data Retention Period: Personal data related to the examination will be retained for three years following the termination of employment.

3. Data Processing for Job Applicants, Applications, and Resumes

(1) Scope of Personal Data Processed: The personal data processed may include the individual's name, date and place of birth, mother's name, address, qualifications, photograph, phone number, email address, and any employer notes about the applicant (if available).

(2) Purpose of Data Processing: The purpose of processing these personal data is to assess applications and candidates, and to enter into an employment contract with the selected applicant. The applicant must be informed if they are not chosen for the position.

(3) Legal Basis for Data Processing: The consent of the data subject.

(4) Recipients of Personal Data or Categories of Recipients: The recipients include Company leaders authorized to exercise employer rights and employees responsible for HR tasks.

(5) Data Retention Period: Personal data will be stored only until the application or candidate evaluation is complete. Personal data of applicants who are not selected must be deleted. Data of those who withdraw their applications must also be deleted.

(6) The employer may retain applications only with the explicit, clear, and voluntary consent of the applicant, provided that retaining the data aligns with a legitimate data processing purpose under applicable laws. This consent should be requested from applicants after the recruitment process concludes.

4. Data Processing Related to Monitoring of Email Account Usage

(1) If the Company provides an email account to the employee, this email account and address may only be used for work-related tasks, allowing employees to communicate with each other or represent the employer in correspondence with clients, other individuals, and organizations.

(2) The employee may not use the email account for personal purposes and may not store personal messages in the account.

(3) The employer is authorized to monitor the full content and usage of the email account regularly, every three months. The legal basis for this data processing is the employer's legitimate interest. The purpose of the monitoring is to verify compliance with the employer's email usage policy and to ensure the employee's adherence to obligations under Sections 8 and 52 of the Labor Code.

(4) The employer’s management or those authorized to exercise employer rights may conduct the monitoring.

(5) If circumstances allow, the employee should be given the opportunity to be present during the monitoring.

(6) Prior to monitoring, the employee must be informed about:

- The employer's legitimate interest in conducting the monitoring,
- Who within the Company is authorized to carry out the monitoring,
- The rules governing the monitoring process, including adherence to the principle of proportionality and the procedural steps involved, and
- The employee’s rights and available remedies regarding data processing related to the monitoring of the email account.

(7) The principle of proportionality must be applied during monitoring. Initially, only the email address and subject line should be examined to determine if the email relates to the employee’s job duties and is not personal. The employer may review the content of non-personal emails without restriction.

(8) If it is determined, contrary to this policy, that the employee has used the email account for personal purposes, the employee must be instructed to promptly delete any personal data. If the employee is absent or uncooperative, the employer will delete the personal data during the monitoring process. The employer may impose disciplinary consequences on the employee for violating this email usage policy.

(9) The employee may exercise the rights described in the chapter on data subject rights in this policy concerning data processing related to the monitoring of the email account.

5. Data Processing Related to Monitoring of Computer, Laptop, and Tablet Usage

(1) The computer, laptop, or tablet provided by the Company to the employee for work purposes may only be used for job-related tasks. Personal use of these devices is prohibited, and the employee must not handle or store any personal data or personal correspondence on them. The employer may monitor the data stored on these devices. Other aspects of monitoring and any disciplinary consequences are governed by the provisions outlined in section 1.4.

6. Data Processing Related to Monitoring of Workplace Internet Usage

(1) The employee is permitted to visit only websites related to their job duties; personal use of the internet at the workplace is prohibited by the employer.

(2) For online registrations completed as part of job duties in the Company’s name, the registration should include an identifier and password associated with the Company. If personal data is required for registration, the Company must initiate its deletion upon termination of the employment relationship.

(3) The employer may monitor the employee’s internet usage at the workplace. The provisions and disciplinary consequences related to this monitoring are governed by section 1.4.

7. Data Processing Related to Monitoring of Corporate Mobile Phone Usage

(1) The employer does not permit personal use of the corporate mobile phone; it is strictly for work-related purposes. The employer may monitor the phone numbers and details of all outgoing calls, as well as data stored on the mobile phone.

(2) The employee is required to notify the employer if they use the corporate mobile phone for personal purposes. In such cases, the employer may request a call detail record from the phone service provider and instruct the employee to anonymize personal call numbers on the document. The employer may also require the employee to cover the costs of personal calls.

(3) Other aspects of monitoring and any disciplinary consequences are governed by the provisions outlined in section 1.4.

8. Data Processing Related to the Use of GPS Navigation System

(1) Legal Basis: The legal basis for using the GPS system is the employer's legitimate interest, with the purpose of organizing work, managing logistics, and monitoring employee duty fulfillment.

(2) Data Processed: License plate number, route taken, distance traveled, and duration of vehicle usage.

(3) Monitoring may only occur during working hours, and employees' geographic location cannot be tracked outside of working hours. Other aspects of monitoring and any disciplinary consequences are governed by the provisions outlined in section 1.4.

9. Data Processing Related to Workplace Access Control

(1) If a non-electronic access control system is operated, information about the data controller and the method of data handling must be displayed.

(2) Scope of Personal Data Processed: Name, address, vehicle license plate number, entry, and exit times.

(3) Legal Basis for Data Processing: The legitimate interest of the employer.

(4) Purpose of Data Processing: Asset protection, contract fulfillment, and monitoring employee duty fulfillment.

(5) Recipients of Personal Data or Categories of Recipients: The Company's authorized management personnel and employees of the Company's security provider, acting as data processors.

(6) Data Retention Period: Personal data will be retained for six months.

10. Data Processing Related to Workplace Video Surveillance

(1) At the Company's headquarters, branch offices, and in areas open for client interactions, an electronic surveillance system is employed to protect human life, physical safety, personal freedom, business secrets, and assets. This system may record video, audio, or both, which means that the recorded behavior of individuals is considered personal data.

(2) Legal Basis: The legal basis for this data processing is the enforcement of the employer’s legitimate interests and the consent of the data subjects.

(3) For areas under surveillance, clear and visible signs must be placed to notify individuals, including third parties, about the presence of the system. Information should be displayed for each camera, explaining that monitoring is conducted for security purposes, the purpose of recording personal data (video and audio), the legal basis for data processing, the location of data storage, retention period, system operator, authorized data access individuals, and details on the rights and remedies of data subjects.

(4) Video and audio recordings of third parties (such as clients, visitors, or guests) entering monitored areas may be made and processed with their consent. Consent can be implied, such as when individuals enter the monitored area after being notified of the surveillance system.

(5) Recorded footage, if not used, may be retained for a maximum of three (3) business days. Use is defined as employing recorded video, audio, or both as evidence in a court or other official proceeding.

(6) Individuals whose rights or legitimate interests are affected by the recording may request, within three business days of the recording, that the data controller retain the recording, providing proof of their right or legitimate interest.

(7) Surveillance cannot be conducted in areas where it would infringe on human dignity, such as dressing rooms, showers, restrooms, medical rooms, or waiting areas attached to them, or in rooms designated for employees to take breaks.

(8) The entire workplace area may be monitored if no one is legally allowed on the premises, such as outside of working hours or on public holidays. In these cases, areas like dressing rooms, restrooms, and designated break rooms may be monitored.

(9) Viewing of data recorded by the electronic surveillance system is permitted only to those legally authorized or to personnel such as the system operator, the employer’s manager and deputy, and the workplace manager for the monitored area, for the purpose of investigating violations and ensuring the system’s proper functioning.

CHAPTER IV
DATA PROCESSING RELATED TO CONTRACTS

1. Processing of Contract Partner Data – Customer and Supplier Records

1) On the legal basis of contract performance, the Company processes personal data of individuals contracted as customers or suppliers, specifically for the purposes of contract formation, fulfillment, termination, and provision of contractual discounts. The processed data includes the natural person's name, birth name, date of birth, mother's name, address, tax identification number, tax number, entrepreneur or agricultural producer identification number, personal ID number, address, headquarters, and branch office address, phone number, email address, website URL, bank account number, customer number (client number, order number), and online identifier (lists of customers, suppliers, loyalty lists). This data processing is lawful even if it is necessary to take steps requested by the data subject prior to contract formation.

The recipients of this personal data include the Company's employees responsible for customer service, accounting, and tax tasks, as well as the Company's data processors. Personal data will be retained for five years following the termination of the contract.

(2) Before commencing data processing, the data subject must be informed that the legal basis for data processing is contract performance. This information may be provided within the contract itself.

(3) The data subject must also be informed if their personal data is transferred to a data processor.

2. Contact Information of Representatives of Corporate Clients, Customers, and Suppliers

(1) Scope of Personal Data Processed: Name, address, phone number, email address, and online identifier of the natural person representative.

(2) Purpose of Data Processing: The purpose of processing these personal data is to fulfill the contract with the Company's corporate partner and to facilitate business communication. The legal basis for this data processing is the data subject's consent.

(3) Recipients of Personal Data or Categories of Recipients: The recipients include the Company's employees responsible for customer service tasks.

(4) Data Retention Period: Personal data will be retained for five years following the termination of the business relationship or the data subject's role as representative.

3. Recording of Customer Service Phone Calls

(1) The Company records phone communications with its customer service to facilitate sales, fulfill service provisions, and provide related information. The legal basis for this data processing is the consent of the data subject.

(2) At the beginning of the call, the caller must be informed about the recording and asked for their consent.

(3) The following data are stored from recorded calls: phone number, call time, recorded audio of the conversation, and any personal data provided during the conversation.

(4) Recipients of Personal Data or Categories of Recipients: The recipients are the Company's employees responsible for customer service tasks.

(5) Recorded phone conversations are retained for five years. Recorded audio can be retrieved based on the phone number and the date of the conversation.

4. Visitor Data Processing on the Company's Website

(1) Cookies: Cookies are short data files placed on the user's computer by the visited website to facilitate or make the online service more convenient. There are various types of cookies, generally divided into two categories. Temporary cookies are only stored on the user's device for a specific session (e.g., for secure identification during online banking), while persistent cookies remain on the computer until deleted by the user (e.g., for website language settings). According to European Commission guidelines, cookies (except those essential for the use of a specific service) may only be placed on a user's device with their consent.

(2) For cookies that do not require user consent, information must be provided during the user's first visit to the website. It is not necessary to display the full cookie information text on the website; a brief summary of the essential points with a link to the full cookie policy is sufficient.

(3) For cookies that require user consent, information may also be provided during the user's first visit if data processing associated with the cookies begins upon accessing the site. If the cookies relate to a function specifically requested by the user, information can appear in connection with the use of that function. In this case, a short summary of the key points is sufficient, with a link to the full cookie policy.

5. Information on the Use of Cookies

(1) In line with common internet practices, our Company uses cookies on its website. A cookie is a small file containing a series of characters that is placed on the visitor's computer when they visit a website. When the visitor returns to the website, the cookie allows the site to recognize their browser. Cookies can store user settings (e.g., chosen language) and other information. They collect information about the visitor and their device, remember individual settings, and can be used for functionalities like online shopping carts. Generally, cookies make it easier to use the website, enhance the online experience for users, serve as an effective information source, allow the website operator to monitor website operation, prevent misuse, and ensure seamless and high-quality services on the website.

(2) During use, our website records and processes the following data about the visitor and the device used for browsing:

- IP address of the visitor,
- Browser type,
- Characteristics of the device's operating system (including the set language),
- Date and time of the visit,
- The (sub)pages, features, or services visited.

(3) Accepting or enabling the use of cookies is not mandatory. You can adjust your browser settings to refuse all cookies or to alert you when a cookie is being sent. Although most browsers automatically accept cookies by default, these settings can generally be modified to prevent automatic acceptance, allowing users to choose each time.

You can find information about cookie settings for the most popular browsers at the following links:

• Google Chrome:

https://support.google.com/accounts/answer/61416?hl=en

• Firefox:

https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop?redirectslug=enable-and-disable-cookies-website-preferences&redirectlocale=en-US

• Microsoft Internet Explorer 11:

https://support.microsoft.com/en-gb/windows/manage-cookies-in-microsoft-edge-view-allow-block-delete-and-use-168dab11-0753-043d-7c16-ede5947fc64d#ie=ie-11

• Microsoft Internet Explorer 10:

https://support.microsoft.com/en-gb/windows/manage-cookies-in-microsoft-edge-view-allow-block-delete-and-use-168dab11-0753-043d-7c16-ede5947fc64d#ie=ie-10-win-7

• Microsoft Internet Explorer 9:

https://support.microsoft.com/en-gb/windows/manage-cookies-in-microsoft-edge-view-allow-block-delete-and-use-168dab11-0753-043d-7c16-ede5947fc64d#ie=ie-9

• Microsoft Internet Explorer 8:

https://support.microsoft.com/en-gb/windows/manage-cookies-in-microsoft-edge-view-allow-block-delete-and-use-168dab11-0753-043d-7c16-ede5947fc64d#ie=ie-8

• Microsoft Edge:

https://support.microsoft.com/en-gb/windows/microsoft-edge-browsing-data-and-privacy-bb8174ba-9d73-dcf2-9b4a-c582b4e640dd

• Safari:

https://support.apple.com/en-us/105082

However, we would like to highlight that certain website features or services may not function properly without cookies.

(4) The cookies used on this website are not capable of identifying the user personally.

(5) Cookies Used on the Company's Website:

Technically Essential Session Cookies
These cookies are necessary for visitors to browse the website smoothly, fully utilize its features, and access services provided through the website—such as remembering actions taken by the visitor during a single session. The data processing duration for these cookies is limited to the visitor's current session; they are automatically deleted from the computer at the end of the session or upon closing the browser.

Data Processed: AVChatUserId, JSESSIONID, portal_referer.
Legal Basis for Data Processing: Section 13/A (3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services.
Purpose of Data Processing: To ensure the proper functioning of the website.
Consent-Based Cookies
These cookies allow the Company to remember the user's choices related to the website. The visitor may prohibit this data processing at any time before or during the use of the service. This data cannot be linked to the user's identifying information and cannot be shared with third parties without the user's consent.

2.1. Usage-Enhancing Cookies

Legal Basis for Data Processing: User consent.
Purpose of Data Processing: To improve the service's effectiveness, enhance the user experience, and make website usage more convenient.
Data Retention Period: 6 months.

2.2. Performance Cookies

Google Analytics Cookies – You can find more information here:
https://support.google.com/analytics/answer/11397207?hl=en

Google AdWords Cookies – More information is available here:
https://business.safety.google/adscookies/

6. Registration on the Company's Website

(1) On the website, individuals registering can provide their consent to the processing of their personal data by checking the designated box. The box must not be pre-checked.

(2) Scope of Personal Data Processed: Name (last name, first name), address, phone number, email address, and online identifier.

(3) Purpose of Data Processing:

- Fulfillment of services provided on the website.
- Communication through electronic, phone, SMS, and postal contact.
- Information about the Company's products, services, contractual terms, and promotions.
- Sending advertising materials electronically and by post.
- Analyzing website usage.

(4) Legal Basis for Data Processing: The data subject’s consent.

(5) Recipients of Personal Data or Categories of Recipients: Company employees responsible for customer service and marketing activities, and employees of the Company’s IT service provider acting as a data processor for hosting services.

(6) Data Retention Period: Until the registration/service is active or until the data subject withdraws their consent (requests deletion).

7. Data Processing Related to Newsletter Service

(1) On the website, individuals registering for the newsletter service can provide their consent by checking the designated box. The box must not be pre-checked. The data subject can unsubscribe from the newsletter at any time by using the "Unsubscribe" feature in the newsletter, or by submitting a written or email request, which constitutes withdrawal of consent. In such cases, all data of the unsubscribing individual must be deleted immediately. The text for information on the newsletter subscription page is provided in Appendix 7 of this Policy.

(2) Scope of Personal Data Processed: Name (last name, first name) and email address.

(3) Purpose of Data Processing:

Sending newsletters about the Company’s products and services.
Sending promotional materials.
(4) Legal Basis for Data Processing: The data subject’s consent.

(5) Recipients of Personal Data or Categories of Recipients: Company employees responsible for customer service and marketing, and employees of the Company’s IT service provider for the purpose of hosting services.

(6) Data Retention Period: Until the newsletter service is active or until the data subject withdraws their consent (requests deletion).

8. Community Guidelines / Data Processing on the Company’s Facebook Page

(1) The Company maintains a Facebook page to promote and introduce its products and services.

(2) Queries submitted on the Company’s Facebook page are not considered official complaints.

(3) The Company does not process personal data published by visitors on its Facebook page.

(4) Visitors are subject to Facebook’s Privacy and Service Terms.

(5) In cases of unlawful or offensive content, the Company reserves the right to remove comments or exclude the user from the page without prior notice.

(6) The Company is not responsible for any unlawful content or comments posted by Facebook users, nor for any errors, interruptions, or issues arising from Facebook's functionality or changes in the platform's operation.

9. Data Processing in the Company's Web Store

(1) Purchases made through the Company's web store constitute a contract, as per Section 13/A of Act CVIII of 2001 on Electronic Commerce Services and Information Society Services, and Government Decree 45/2014 (II. 26.) on detailed rules of contracts between consumers and businesses. The legal basis for data processing in web store purchases is contract fulfillment.

(2) The Company may process the personal identification data and address of individuals who register and make purchases in the web store, for the purpose of contract formation, content definition, modification, performance monitoring, invoicing, and enforcement of claims, based on Section 13/A(1) of Act CVIII of 2001. The legal basis for processing the individual's phone number, email address, bank account number, and online identifier is consent.

(3) For invoicing, the Company may process personal identification data, address, as well as the date, duration, and location of service use, based on Section 13/A(2) of Act CVIII of 2001.

(4) Recipients of Personal Data or Categories of Recipients: Company employees responsible for customer service and marketing, employees of the Company's accounting and tax service provider for tax and accounting compliance, employees of the Company's IT service provider for hosting services, and employees of the courier service provider for handling delivery data (name, address, phone number).

(5) Data Retention Period: Personal data will be retained for the duration of the registration/service or until the data subject withdraws their consent (requests deletion). For purchases, data will be retained for five years following the year of purchase.

10. Data Processing Related to Organizing Prize Draws

(1) If the Company organizes a prize draw (according to Section 23 of Act XXXIV of 1991), it may process the name, address, phone number, email address, and online identifier of the participating natural person with their consent. Participation in the prize draw is voluntary.

(2) Purpose of Data Processing: To determine and notify the winner of the prize draw and to send the prize. The legal basis for data processing is the consent of the data subject.

(3) Recipients of Personal Data or Categories of Recipients: Employees of the Company responsible for customer service, employees of the Company's IT service provider responsible for server services, and employees of the courier service provider.

(4) Data Retention Period: Until the finalization of the prize draw.

11. Data Processing for Direct Marketing Purposes

(1) Unless otherwise specified by law, advertisements may be sent directly to a natural person as an advertising recipient (direct marketing) — especially via electronic mail or other equivalent individual communication tools — only if the recipient has provided prior, explicit consent, as outlined in Act XLVIII of 2008.

(2) Scope of Personal Data Processed for Advertising Purposes: Name, address, phone number, email address, and online identifier of the natural person.

(3) Purpose of Data Processing: To conduct direct marketing activities related to the Company's services, which includes the regular or occasional sending of advertising materials, newsletters, and current offers to the contact details provided during registration, either in printed form (postal) or electronically (email).

(4) Legal Basis for Data Processing: The consent of the data subject.

(5) Recipients of Personal Data or Categories of Recipients: Company employees responsible for customer service tasks, employees of the Company's IT service provider responsible for server services, and postal employees for physical delivery.

(6) Data Retention Period: Until the data subject withdraws their consent.

CHAPTER V
DATA PROCESSING BASED ON LEGAL OBLIGATIONS

1. Data Processing for Fulfilling Tax and Accounting Obligations

(1) The Company processes the legally required personal data of natural persons with whom it enters into business relationships as customers or suppliers, for the purpose of fulfilling legal tax and accounting obligations (such as bookkeeping and taxation). The processed data, as mandated by Act CXXVII of 2017 on Value Added Tax (Sections 169 and 202), includes, in particular, tax number, name, address, and tax status. According to Act C of 2000 on Accounting (Section 167), this data includes name, address, identification of the individual or organization authorizing the transaction, the voucher issuer, executor of the order, and the signature of the verifier (as applicable within the organization). Further data includes the signature of the receiver on inventory records and cash management documents, the signature of the payer on receipts, and the entrepreneurial or agricultural producer license number and tax identification number, as required by Act CXVII of 1995 on Personal Income Tax.

(2) Data Retention Period: Personal data will be retained for eight years following the termination of the legal relationship that serves as the legal basis for the processing.

(3) Recipients of Personal Data: Company employees and data processors responsible for handling the Company's tax, accounting, payroll, and social security tasks.

2. Data Processing by Payers

(1) Based on legal obligations, the Company processes the personal data of employees, family members, contractors, and other beneficiaries with whom it has a payer relationship (under Section 7.§ 31 of Act CL of 2017 on the Rules of Taxation, or "Art.") for the purposes of fulfilling statutory tax and contribution obligations (taxes, tax advances, contributions, payroll, social security, and pension management). The scope of processed data, as defined by Art. Section 50.§, includes personal identifiers (such as previous names and titles), gender, nationality, tax identification number, social security number (TAJ number), and, where stipulated by tax laws, health information (under Section 40 of the Personal Income Tax Act) and union membership (under Section 47(2)(b) of the Personal Income Tax Act) for tax and contribution fulfillment.

(2) Data Retention Period: Personal data is retained for eight years following the termination of the legal relationship that serves as the legal basis for processing.

(3) Recipients of Personal Data: Employees and data processors handling the Company's tax, payroll, and social security (payer) tasks.

3. Data Processing Related to Archival Materials of Permanent Value

(1) Based on legal obligations, the Company processes documents deemed of permanent value under Act LXVI of 1995 on Public Records, Public Archives, and the Protection of Private Archives (the Archival Act), to preserve archival materials for future generations. Data Retention Period: Until the transfer to a public archive.

(2) Other questions regarding data recipients and processing are governed by the Archival Act.

4. Data Processing for Anti-Money Laundering Obligations

(1) The Company, based on legal obligations, processes the personal data of clients, their representatives, and beneficial owners as required by Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing ("Pmt.") to prevent and combat money laundering and terrorism financing. The data processed includes: a) full name, b) birth name, c) nationality, d) place and date of birth, e) mother's maiden name, f) address or place of residence, g) type and number of identification document, h) official address document number, and copies of provided documents (Section 7.§ of Pmt.).

(2) Recipients of Personal Data: Employees responsible for client service, the Company's manager, and the Company's designated person under Pmt.

(3) Data Retention Period: Eight years from the termination of the business relationship or the completion of the transaction (Pmt. Section 56.§(2)).

CHAPTER VI
SUMMARY OF DATA SUBJECT RIGHTS

In this chapter, we provide a brief overview of the data subject's rights for clarity and transparency. Detailed information on exercising these rights is provided in the following chapter.

Right to Prior Information
The data subject has the right to receive information about facts and details related to data processing before it begins.
(Regulation Articles 13-14)
Details are provided in the next chapter.

Right of Access
The data subject has the right to receive confirmation from the Data Controller regarding whether their personal data is being processed. If such processing is taking place, the data subject has the right to access the personal data and related information as defined in the Regulation.
(Regulation Article 15)
Details are provided in the next chapter.

Right to Rectification
The data subject has the right to request the Data Controller to correct inaccurate personal data concerning them without undue delay. Considering the purpose of data processing, the data subject also has the right to request the completion of incomplete personal data, including through a supplementary statement.
(Regulation Article 16)

Right to Erasure ("Right to be Forgotten")
1. The data subject has the right to request the Data Controller to delete their personal data without undue delay, and the Data Controller is obliged to erase the personal data without undue delay if one of the reasons specified in the Regulation applies.
(Regulation Article 17)
Details are provided in the next chapter.

Right to Restriction of Processing
The data subject has the right to request the Data Controller to restrict data processing if the conditions specified in the Regulation are met.
(Regulation Article 18)
Details are provided in the next chapter.

Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing
The Data Controller must inform all recipients with whom personal data has been shared of any rectifications, deletions, or restrictions on data processing unless this proves impossible or requires disproportionate effort. Upon request, the Data Controller shall inform the data subject of these recipients.
(Regulation Article 19)

Right to Data Portability
Under the conditions outlined in the Regulation, the data subject has the right to receive personal data they have provided to a Data Controller in a structured, commonly used, machine-readable format and has the right to transfer this data to another Data Controller without hindrance from the original Data Controller.

Right to Object
The data subject has the right to object at any time, on grounds relating to their particular situation, to the processing of personal data concerning them based on Article 6(1)(e) (processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority) or (f) (processing necessary for the purposes of the legitimate interests pursued by the Data Controller or a third party).
(Regulation Article 21)
Details are provided in the next chapter.

Right Not to Be Subject to Automated Decision-Making, Including Profiling
The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.
(Regulation Article 22)
Details are provided in the next chapter.

Restrictions
Union or Member State law applicable to the Data Controller or Data Processor may restrict the rights and obligations referred to in Articles 12–22 and Article 34 through legislative measures.
(Regulation Article 23)
Details are provided in the next chapter.

Right to Be Informed of a Data Breach
If a data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the breach without undue delay.
(Regulation Article 34)
Details are provided in the next chapter.

Right to Lodge a Complaint with a Supervisory Authority (Right to Legal Remedy)
The data subject has the right to lodge a complaint with a supervisory authority, particularly in the Member State of their habitual residence, place of work, or place of the alleged infringement, if they believe that the processing of personal data concerning them infringes the Regulation.
(Regulation Article 77)
Details are provided in the next chapter.

Right to an Effective Judicial Remedy Against a Supervisory Authority
Every natural and legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them or if the supervisory authority does not handle a complaint or fails to inform the data subject within three months about the progress or outcome of the complaint.
(Regulation Article 78)
Details are provided in the next chapter.

Right to an Effective Judicial Remedy Against the Data Controller or Data Processor
The data subject has the right to an effective judicial remedy if they consider that their rights under the Regulation have been infringed due to the improper processing of their personal data.
(Regulation Article 79)
Details are provided in the next chapter.

CHAPTER VII
DETAILED INFORMATION ON THE RIGHTS OF THE DATA SUBJECT

Right to Prior Information
The data subject has the right to receive information about facts and details related to data processing before the processing begins.

A) Information to Be Provided When Personal Data Is Collected from the Data Subject

If personal data concerning the data subject is collected directly from them, the Data Controller shall provide the following information at the time of data collection:

a) The identity and contact details of the Data Controller and, if applicable, the representative of the Data Controller;
b) Contact details of the Data Protection Officer, if available;
c) The purpose of the intended data processing and the legal basis for processing;
d) In cases where processing is based on Article 6(1)(f) of the Regulation (processing based on legitimate interests), the legitimate interests pursued by the Data Controller or a third party;
e) Where applicable, the recipients or categories of recipients of the personal data;
f) Where applicable, whether the Data Controller intends to transfer personal data to a third country or international organization, and the existence or absence of an adequacy decision by the Commission, or in the case of data transfers specified under Article 46, 47, or 49(1)(2) of the Regulation, reference to appropriate or suitable safeguards and the means of obtaining a copy or where they have been made available.
In addition to the information mentioned in point 1, the Data Controller shall, at the time of data collection, inform the data subject of the following supplementary information to ensure fair and transparent processing:

a) The duration for which personal data will be stored, or if not possible, the criteria used to determine that period;
b) The data subject's rights to request access, rectification, erasure, restriction of processing, objection to processing, and data portability regarding their personal data;
c) Where processing is based on consent under Article 6(1)(a) or Article 9(2)(a) of the Regulation, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d) The right to lodge a complaint with a supervisory authority;
e) Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and whether the data subject is obliged to provide the personal data, as well as the possible consequences of failure to provide such data;
f) The existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the Regulation, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the anticipated consequences of such processing for the data subject.
If the Data Controller intends to further process the personal data for a purpose other than that for which the data was collected, the Data Controller shall inform the data subject of this different purpose and any relevant supplementary information as mentioned in point 2 before the further processing.

Points 1-3 do not apply if and to the extent that the data subject already has the information.
(Regulation Article 13)

B) Information to Be Provided When Personal Data Is Not Collected from the Data Subject

1. If personal data has not been obtained directly from the data subject, the Data Controller shall provide the data subject with the following information:

a) The identity and contact details of the Data Controller and, if applicable, the Data Controller's representative;
b) Contact details of the Data Protection Officer, if available;
c) The purpose and legal basis for the intended processing of personal data;
d) The categories of personal data concerned;
e) The recipients or categories of recipients of the personal data, if applicable;
f) Where applicable, if the Data Controller intends to transfer personal data to a recipient in a third country or international organization, including whether a Commission adequacy decision exists or, in the absence of such a decision, reference to appropriate safeguards (such as those in Articles 46, 47, or 49(1) of the Regulation) and the means of obtaining a copy or access to these safeguards.

2. In addition to the information in point 1, the Data Controller shall provide the following supplementary information necessary to ensure fair and transparent processing for the data subject:

a) The duration for which personal data will be stored, or, if not possible, the criteria used to determine that period;
b) If processing is based on Article 6(1)(f) of the Regulation (legitimate interest), a description of the legitimate interests pursued by the Data Controller or a third party;
c) The data subject's rights to request access to, rectification or erasure of, restriction of processing, and to object to processing of their personal data, as well as the right to data portability;
d) Where processing is based on consent (under Article 6(1)(a) or Article 9(2)(a)), the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before withdrawal;
e) The right to lodge a complaint with a supervisory authority;
f) The source of the personal data, and if applicable, whether it originated from publicly accessible sources;
g) The existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4), and meaningful information about the logic involved, as well as the significance and anticipated consequences of such processing for the data subject.

3. The Data Controller shall provide the information described in points 1 and 2:

a) Within a reasonable period after obtaining the personal data, but at the latest within one month;
b) If the personal data is used to communicate with the data subject, at the latest at the time of the first communication; or
c) If the personal data is disclosed to another recipient, at the latest at the time of the first disclosure.

4. If the Data Controller intends to process personal data for a purpose other than that for which it was collected, it must inform the data subject of this different purpose and any relevant supplementary information mentioned in point 2 before the further processing.

5. Points 1-4 do not apply if and to the extent that:

a) The data subject already has the information;
b) The provision of such information proves impossible or would involve disproportionate effort, particularly in cases of data processing for public interest archival, scientific or historical research, or statistical purposes under the conditions and safeguards of Article 89(1) of the Regulation, or if

fulfilling the obligation referred to in paragraph (1) of this article would likely render impossible or seriously impair the achievement of the objectives of that processing. In such cases, the Data Controller shall take appropriate measures to protect the data subject's rights, including making the information publicly available;
c) The acquisition or disclosure of personal data is explicitly laid down by Union or Member State law to which the Data Controller is subject, and that law provides appropriate safeguards for the data subject's legitimate interests; or
d) The personal data must remain confidential due to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.
(Regulation Article 14)

Right of Access by the Data Subject

1. The data subject has the right to obtain confirmation from the Data Controller as to whether personal data concerning them is being processed. If processing is ongoing, the data subject has the right to access their personal data and the following information:

a) The purposes of the processing;
b) The categories of personal data concerned;
c) The recipients or categories of recipients to whom the personal data has been or will be disclosed, including in particular recipients in third countries or international organizations;
d) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) The right to request rectification or erasure of personal data or restriction of processing concerning the data subject, or to object to such processing;
f) The right to lodge a complaint with a supervisory authority;
g) If the data was not collected from the data subject, any available information as to its source;
h) The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the Regulation, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the anticipated consequences of such processing for the data subject.

2. If personal data is transferred to a third country or an international organization, the data subject has the right to be informed about the appropriate safeguards related to the transfer pursuant to Article 46 of the Regulation.

3. The Data Controller shall provide a copy of the personal data undergoing processing to the data subject. For any additional copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. If the data subject makes the request electronically, the information shall be provided in a commonly used electronic format, unless otherwise requested by the data subject. The right to obtain a copy shall not adversely affect the rights and freedoms of others.
(Regulation Article 15)

Right to Erasure ("Right to be Forgotten")

1. The data subject has the right to have the Data Controller erase their personal data without undue delay, and the Data Controller is obligated to erase personal data without undue delay if any of the following grounds apply:
a) The personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
b) The data subject withdraws consent on which the processing is based according to Article 6(1)(a) or Article 9(2)(a) of the Regulation, and there is no other legal ground for the processing;

c) The data subject objects to the processing pursuant to Article 21(1) of the Regulation, and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
d) The personal data has been processed unlawfully;
e) The personal data must be erased to comply with a legal obligation under Union or Member State law applicable to the Data Controller;
f) The personal data was collected in relation to the offer of information society services referred to in Article 8(1) of the Regulation.

2. If the Data Controller has made the personal data public and is obliged to erase it under point 1, the Data Controller, taking into account available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested the deletion of any links to, or copies or replications of, such personal data.

3. Points 1 and 2 do not apply to the extent that processing is necessary:

a) For exercising the right of freedom of expression and information;
b) For compliance with a legal obligation requiring processing under Union or Member State law to which the Data Controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
c) For reasons of public interest in the area of public health, in accordance with Article 9(2)(h) and (i), and Article 9(3) of the Regulation;
d) For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the Regulation, insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e) For the establishment, exercise, or defense of legal claims.
(Regulation Article 17)

Right to Restriction of Processing

1. The data subject has the right to obtain restriction of processing from the Data Controller if any of the following conditions apply:

a) The data subject contests the accuracy of the personal data, in which case the restriction applies for a period enabling the Data Controller to verify the accuracy of the personal data;
b) The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of its use instead;
c) The Data Controller no longer needs the personal data for processing purposes, but the data subject requires it for the establishment, exercise, or defense of legal claims; or
d) The data subject has objected to processing pursuant to Article 21(1) of the Regulation; in this case, the restriction applies pending verification of whether the Data Controller’s legitimate grounds override those of the data subject.

2. If processing has been restricted under point 1, such personal data, except for storage, shall only be processed with the data subject's consent or for the establishment, exercise, or defense of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.

3. The Data Controller shall inform the data subject who requested the restriction of processing under point 1 before lifting the restriction on processing.
(Regulation Article 18)

Right to Data Portability

1. The data subject has the right to receive the personal data concerning them, which they have provided to a Data Controller, in a structured, commonly used, and machine-readable format, and has the right to transmit that data to another Data Controller without hindrance from the original Data Controller, provided that:

a) The processing is based on consent under Article 6(1)(a) or Article 9(2)(a) of the Regulation, or on a contract under Article 6(1)(b); and
b) The processing is carried out by automated means.

2. When exercising their right to data portability under point 1, the data subject has the right to have the personal data transmitted directly from one Data Controller to another, where technically feasible.

3. Exercising the right to data portability shall not adversely affect the rights and freedoms of others, nor shall it conflict with the right to erasure under Article 17 of the Regulation. This right does not apply where processing is necessary for performing a task in the public interest or in the exercise of official authority vested in the Data Controller.

4. The right outlined in point 1 must not infringe on the rights and freedoms of others.
(Regulation Article 20)

Right to Object

1. The data subject has the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them based on Article 6(1)(e) (processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority) or Article 6(1)(f) (processing necessary for the purposes of the legitimate interests pursued by the Data Controller or a third party), including profiling based on these provisions. In such cases, the Data Controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing that override the data subject's interests, rights, and freedoms, or for the establishment, exercise, or defense of legal claims.

2. Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to processing of their personal data for such marketing, which includes profiling to the extent related to direct marketing.

3. If the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. The data subject must be explicitly informed of the rights mentioned in points 1 and 2 (the right to object to processing based on public interest or legitimate interest, and the right to object to processing for direct marketing purposes) no later than at the time of the first contact with them. This information must be presented clearly and separately from any other information.

5. In connection with information society services and notwithstanding Directive 2002/58/EC, the data subject may exercise their right to object by automated means using technical specifications.

6. Where personal data is processed for scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation, the data subject, on grounds relating to

their particular situation, shall have the right to object to processing of their personal data, unless the processing is necessary for the performance of a task carried out for reasons of public interest.
(Regulation Article 21)

Automated Individual Decision-Making, Including Profiling

1. The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

2. Point 1 does not apply if the decision:

a) Is necessary for entering into, or performance of, a contract between the data subject and the Data Controller;
b) Is authorized by Union or Member State law applicable to the Data Controller, which also lays down suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests; or
c) Is based on the data subject's explicit consent.

3. In the cases referred to in points 2(a) and (c), the Data Controller must implement suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests. These include the right to obtain human intervention from the Data Controller, to express their point of view, and to contest the decision.

4. Decisions referred to in point 2 cannot be based on special categories of personal data referred to in Article 9(1) of the Regulation, unless Article 9(2)(a) or (g) applies and suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests have been implemented.
(Regulation Article 22)

Restrictions

1. Union or Member State law applicable to the Data Controller or Data Processor may restrict the scope of the rights and obligations outlined in Articles 12–22 and Article 34 of the Regulation, as well as the rights and obligations in Article 5, by means of legislative measures, provided that the restriction respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society to safeguard:
a) National security;
b) Defense;
c) Public security;
d) The prevention, investigation, detection, or prosecution of criminal offenses, or the execution of criminal penalties, including the protection against and prevention of threats to public security;
e) Other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary, and taxation matters, public health, and social security;
f) The independence of the judiciary and judicial proceedings;
g) The prevention, investigation, detection, and prosecution of breaches of ethics in regulated professions;
h) Monitoring, inspection, or regulatory functions connected, even occasionally, to the exercise of official authority in the cases referred to in points (a)–(e) and (g);
i) The protection of the data subject or the rights and freedoms of others;
j) The enforcement of civil law claims.

2. The legislative measures referred to in point 1 may include specific provisions, where relevant, at least with regard to:
a) The purposes of the processing or categories of processing;
b) The categories of personal data concerned;
c) The scope of the introduced restrictions;
d) Safeguards to prevent abuse or unlawful access or transfer;
e) Specification of the Data Controller or categories of Data Controllers;
f) The storage periods and applicable safeguards, taking into account the nature, scope, and purposes of the processing or categories of processing;
g) The risks to the rights and freedoms of data subjects; and
h) The rights of data subjects to be informed about the restriction, unless this would adversely affect the purpose of the restriction.
(Regulation Article 23)

Notification of the Data Subject About a Personal Data Breach

1. If a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the personal data breach without undue delay.

2. The information provided to the data subject as per point 1 shall describe the nature of the personal data breach in clear and plain language, and include at least the information and measures referred to in Article 33(3)(b), (c), and (d) of the Regulation.

3. The data subject need not be informed in accordance with point 1 if any of the following conditions are met:

a) The Data Controller has implemented appropriate technical and organizational protection measures, and these measures were applied to the personal data affected by the personal data breach—particularly those measures, such as encryption, which render the personal data unintelligible to any person who is not authorized to access it;
b) The Data Controller has taken subsequent measures to ensure that the high risk to the data subject's rights and freedoms referred to in point 1 is no longer likely to materialize;
c) Notifying the data subject would involve disproportionate effort. In such cases, public communication or a similar measure shall be made to inform data subjects in an equally effective manner.

4. If the Data Controller has not yet informed the data subject of the personal data breach, the supervisory authority, after considering the likelihood of a high risk, may require the Data Controller to notify the data subject or may determine that one of the conditions referred to in point 3 is met.
(Regulation Article 34)

Right to Lodge a Complaint with a Supervisory Authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of their habitual residence, place of work, or place of the alleged infringement, if they consider that the processing of personal data relating to them infringes this Regulation.
2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint, including the possibility of a judicial remedy pursuant to Article 78 of the Regulation.
(Regulation Article 77)

Right to an Effective Judicial Remedy Against a Supervisory Authority

1. Without prejudice to any other administrative or non-judicial remedy, every natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, every data subject shall have the right to an effective judicial remedy if the competent supervisory authority under Articles 55 or 56 does not handle a complaint or does not inform the data subject within three months about the progress or outcome of a complaint lodged under Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority that was preceded by an opinion or decision by the Board under the consistency mechanism, the supervisory authority shall submit that opinion or decision to the court.
(Regulation Article 78)

Right to an Effective Judicial Remedy Against a Controller or Processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority under Article 77, every data subject shall have the right to an effective judicial remedy where they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

2. Proceedings against a Controller or Processor shall be brought before the courts of the Member State where the Controller or Processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has their habitual residence unless the Controller or Processor is a public authority of a Member State acting in the exercise of its public powers.
(Regulation Article 79)

Chapter VIII
Submission of Requests by the Data Subject and Actions by the Data Controller

1. The Data Controller shall inform the data subject without undue delay and in any event within one month of receipt of the request regarding actions taken in response to the exercise of their rights.

2. If necessary, considering the complexity and number of requests, this period may be extended by an additional two months. The Data Controller shall inform the data subject of any such extension within one month of receiving the request, along with the reasons for the delay.

3. If the data subject submitted the request electronically, the response should, where possible, be provided electronically unless the data subject requests otherwise.

4. If the Data Controller does not take action based on the data subject's request, it shall inform the data subject without undue delay and at the latest within one month of receiving the request of the reasons for not taking action. The data subject shall also be informed of the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. The Data Controller shall provide the information required under Articles 13 and 14 of the Regulation and any actions taken in response to the data subject’s rights (under Articles 15–22 and 34) free of charge. However, if a data subject's request is manifestly unfounded or excessive — particularly due to its repetitive nature — the Data Controller may: a) Charge a fee of 6,350 HUF to cover administrative costs associated with providing the information or performing the requested action, or b) Refuse to act on the request. The burden of demonstrating the manifestly unfounded or excessive nature of the request lies with the Data Controller.

6. If the Data Controller has reasonable doubts about the identity of the natural person making the request, it may request additional information necessary to confirm the individual’s identity.

Homoky Hotels Tiliana Hotel 2018.