Company name: Petit Bois Füred

Place of business: 7, Táncsics Mihály utca, 8230 Balatonfüred.

Tax number: 32401431-2-42

Company registration number: 01-09-422190

Privacy policy

Effective: 1 November 2024.

1. BEVEZETÉS

The Petit Bois Hotel Management Ltd., the operator of Petit Bois Füred (hereinafter referred to as: Hotel), as the Data Controller, pays special attention to the protection of personal data, compliance with mandatory legal provisions, safe and fair data management in the activities of its customers, guests and visitors to the website.

Data of the Data Controller:

Company name: Petit Bois Szállodaüzemeltető Kft.

Registered office: 1151 Budapest, Mogyoród útja 12-14.

Tax number: 32401431-2-42

Company registration number: 01-09-422190

Email: info@petitbois.hu

Website: www.petitbois.hu

Tel: +36-30-258-9371

Internal Data Protection Officer: Péter Laki

The Data Controller shall in all cases process the personal data provided to it in compliance with the applicable Hungarian and European legislation and ethical requirements, and shall in all cases take the technical and organisational measures necessary for the proper and secure processing of the data.

This Policy has been drawn up in compliance with the following legislation in force:

• Act CXIX of 1995 on the Processing of Name and Address Data for Research and Direct Marketing Purposes

• Act CVIII of 2001 on certain aspects of electronic commerce services and information society services

• Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Economic Advertising Activities

• Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information

• Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46

The Data Controller undertakes to unilaterally comply with this Policy and asks its customers to accept the provisions of this Policy by means of a notice on its website. The Data Controller reserves the right to change its Privacy Policy. If the policy is amended, the updated text will be made public.

The current version of the Privacy Policy is available on the website www.petitbois.hu and in hard copy at the reception desk of the Hotel.

This notice regulates the data management activities related to the services provided by the hotel Petit Bois Füred, located at 7, Táncsics Mihály Street, 8230 Balatonfüred, and accessible through the website.

2. INTERPRETATIVE PROVISIONS

In our policy, data protection terms have the following meanings:

- dataset: the set of data managed in a single register;

- 'processor' means a natural or legal person or an unincorporated body which processes data on the basis of a contract, including a contract concluded pursuant to a legal provision;

- 'data controller' means the public sector body which has produced the data of public interest which must be made public by electronic means or in the course of whose activities the data were generated;

- data processing: any operation or set of operations which is performed upon data, regardless of the procedure used, in particular any collection, recording, recording, organisation, storage, alteration, use, retrieval, disclosure, transmission, alignment or combination, blocking, erasure or destruction of data, prevention of their further use, taking of photographs, sound recordings or images and physical features which can be used to identify a person (e.g. fingerprints, palm prints, DNA samples, iris scans);

- controller: the natural or legal person or unincorporated body which, alone or jointly with others, determines the purposes for which the data are to be processed, takes and implements decisions regarding the processing (including the means used) or implements them with the processor;

- data provider: a public sector body which, if the data controller does not publish the data itself, publishes the data submitted to it by the data controller on a website;

- data marking: the marking of data with an identification mark to distinguish it;

- transfer: making data available to a specified third party;

- erasure: making data unrecognisable in such a way that it is no longer possible to recover it;

- personal data breach: unlawful processing or handling of personal data, in particular unauthorised access, alteration, disclosure, transmission, disclosure, erasure or destruction, accidental destruction or accidental damage.

- data blocking: the marking of data with an identification mark for the purpose of limiting its further processing permanently or for a limited period of time;

- criminal personal data: personal data relating to the criminal offence or the criminal proceedings, obtained in the course of or prior to criminal proceedings, by the authorities competent to prosecute or investigate criminal offences, and by the law enforcement authorities, which can be linked to the data subject, and personal data relating to the criminal record;

- EEA State: a Member State of the European Union and another State party to the Agreement on the European Economic Area, and a State whose nationals enjoy the

same status as nationals of a State party to the Agreement on the European Economic Area under an international treaty between the European Union and its Member States and a State not party to the Agreement on the European Economic Area;

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

- third country: any state that is not an EEA state;

- third party: a natural or legal person or unincorporated body other than the data subject, the controller or the processor;

- consent: a voluntary and explicit indication of the data subject's wishes, based on adequate information, by which he or she gives his or her unambiguous agreement to the processing of personal data concerning him or her.

processing of personal data concerning him or her, either in full or in relation to specific operations;

- Binding Corporate Rules: an internal data protection policy adopted by a controller or a group of controllers operating in several countries, including at least one EEA country, and approved by the National Authority for Data Protection and Freedom of Information (hereinafter "the Authority"), which is binding on the controller or group of controllers and which ensures the protection of personal data in the case of transfers to third countries by means of a unilateral undertaking by the controller or group of controllers;

- public interest data: any data not covered by the concept of public interest data, the disclosure, disclosure or making available of which is required by law to be in the public interest;

- special data:

• personal data revealing racial or ethnic origin, nationality, political opinions or opinions, religious or philosophical beliefs, membership of an interest group or membership of a representative body, sex life,

• personal data concerning health, pathological addiction and personal data concerning criminal offences;

- disclosure: making the data available to anyone;

- personal data: data which can be associated with the data subject, in particular the name, the identification mark and one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity, and the conclusions which can be drawn from the data concerning the data subject;

- objection: a statement by the data subject objecting to the processing of his or her personal data and requesting the cessation of the processing or the deletion of the processed data;

• personal data revealing racial or ethnic origin, nationality, political opinions or opinions, religious or philosophical beliefs, membership of an interest group or membership of a representative body, sex life,

• personal data revealing racial or ethnic origin, nationality, political opinions or opinions, religious or philosophical beliefs, membership of an interest group or membership of a representative body, sex life,

- data processing: the performance of technical tasks related to data processing operations, irrespective of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data;

- data destruction: the complete physical destruction of the data medium containing the data;

• personal data concerning health, pathological addiction and personal data concerning criminal offences.

• personal data concerning health, pathological addiction and personal data concerning criminal offences;

- data of public interest : information or knowledge, in whatever form or by whatever means, which is held by a body or person performing a State or local government task or other public task defined by law and which relates to its activities or arises in the course of the performance of its public task, but which is not personal data, irrespective of the way in which it is handled, whether or not it is of a specific or collective nature, in particular data concerning the powers, competences, organisation, structure, professional activities, including an assessment of their effectiveness, the types of data held and the legislation governing their operation, as well as data concerning management and contracts concluded;

3. DATA PROCESSING SUB-POLICIES

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

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

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

The processing must ensure that the data are accurate, complete and, where necessary for the purposes for which they are processed, kept up to date, and that the data subject can be identified only for the time necessary for the purposes for which they are processed.

The processing of personal data shall be considered fair and lawful if, in order to ensure the freedom of expression of the data subject, the person who wishes to know the opinion of the data subject visits the data subject at his or her place of residence or stay, provided that the personal data of the data subject are processed in

accordance with the provisions of this Act and the personal inquiry is not for commercial purposes. The personal inquiry may not take place on a public holiday within the meaning of the Labour Code.

Personal data may be processed if the data subject consents to it or if it is ordered by law or - on the basis of a law, within the scope specified therein - by a local government decree for a purpose in the public interest (mandatory processing).

Personal data may be processed only for specified purposes, for the exercise of rights and the performance of obligations. The processing must comply with this purpose at all stages.

Only personal data which is necessary for the purpose of the processing, is adequate for the purpose, and is processed only to the extent and for the duration necessary for the purpose. Personal data may be transferred and the different processing operations may be combined where the data subject has given his or her consent or where the law permits it and where the conditions for processing are fulfilled for each individual personal data.

Personal data may be transferred from the country to a controller or processor in a third country, irrespective of the data medium or the means of data transfer, if the data subject has given his or her explicit consent or if the law allows it and the third country ensures an adequate level of protection for the processing of the personal data transferred.

In the case of mandatory data processing, the purposes and conditions of the processing, the scope and availability of the data to be processed, the duration of the processing and the identity of the controller are determined by the law or government regulation imposing the processing.

The law may order the disclosure of personal data in the public interest, by expressly indicating the scope of the data. In all other cases, disclosure requires the consent of the data subject, or in the case of sensitive data, written consent. In case of doubt, it shall be presumed that the data subject has not given his or her consent.

The consent of the data subject shall be deemed to be given in respect of the data communicated by him or her in the course of his or her public activities or transmitted by him or her for the purpose of making them public.

In a procedure initiated at the request of the data subject, his or her consent to the processing of the data should be presumed. This fact shall be brought to the attention of the data subject.

The data subject may also give his consent in the context of a written contract with the Data Controller in order to fulfill the provisions of the contract. In this case, the contract must contain all information that the data subject must know from the point of view of the processing of personal data, in particular the definition of the data to be processed, the duration of the data processing, the purpose of use, the transmission of the data, the use of a data processor.

The contract must clearly state that, by signing, the data subject consents to the processing of his/her data as specified in the contract.

The right to the protection of personal data and the privacy rights of the person concerned cannot be violated by other interests related to data management,

including the disclosure of data of public interest, unless the law makes an exception.

4. BASICS OF DATA MANAGEMENT

In the course of its activities, the Data Controller handles personal data in all cases based on law or voluntary consent. In some cases, data management, in the absence of consent, is based on other legal grounds or in accordance with Art. CXII of 2011. is based on § 6 of the Act.

5. SCOPE OF ACTIVITIES AND DATA AFFECTED BY DATA MANAGEMENT

5.1 Request for quotation

The processed data are as follows: Full name*, Email address*, Telephone number*, Postal code*, City*, Street*, house number*, Date of arrival*, Date of departure*, Number of adults*, Number of children 0 - 3.99*, Number of children 4 - 11.99*, Note (baby bed, etc.)

Purpose of data management: Giving the exact offer, preparing the reservation

Legal basis for data management: Consent (GDPR Article 6 (1) point a)

Duration of data management:

- in the event of a successful request for an offer, according to the rules for booking,

- in case of rejection of the offer, until the day of rejection,

- if no response to the offer is received, until the day after the end of the binding offer

No data transmission takes place

During the request for an offer related to a room reservation via the website, the data subject will voluntarily provide the Data Controller with the purpose of providing the Data Controller with a price offer. The activity and process involved in data management are as follows:

o By clicking on the "REQUEST FOR QUOTATION" menu item on the website, the data subject goes to the given page, where he can enter the data specified in point 5.1. After entering the data, the data subject can send the data to the Data Controller by pressing the "SEND" button.

The data sent to the Data Controller is handled by the Data Controller's Receptionist/Room Reservation employees with the help of the hotelsystem program/PMS/SabeeApp hotel software, who record the received data and develop an offer for the data subject, which is sent to him by e-mail.

5.2 Room reservation

The processed data are as follows: Full name*, Email address*, Telephone number*, Postal code*, City*, Street, house number*, Arrival date*, Departure date*, Number of adults

Purpose of data management: Providing the service, fulfilling the room reservation

Legal basis for data management:

Contract performance (GDPR Article 6 (1) point b)

Consent (Article 6(1)(a) GDPR)

Duration of data management: The personal data received during the reservation will be processed for the duration of the contractual relationship with the data subject, except for: data to be kept for 8 years based on Act C of 2000 on accounting, and CL. 2017 on taxation. data to be kept by law until the last day of the 5th year following the relevant year.

Data will be transferred to the Sabeeapp hotel management system for the purpose of operating the online reservation system.

Online booking sites and travel agencies are considered independent data controllers, in this process no data processor is used.

The activity and process involved in data management are as follows:

o If the data subject accepts the offer and informs the Data Controller about this orally or in writing, the Data Controller will take steps related to the room reservation.

o On behalf of the Data Controller, the receptionist (/room reservation) employee working with him enters the data provided by the data subject into the hotelsystem/PMS/SabeeApp program and connects them with the given room of the Hotel with the help of this program, thus creating the room reservation.

The employee with the job title defined above will notify the person concerned in writing about the reservation of the room.

5.3. Check in and the reporting form

The processed data are as follows: Full name*, Postal code, City*, Street*, House number*, Citizenship*, Date of birth*, Passport or Identity card number*, Tax number in the case of a company* Purpose of data management: Maintaining contact and fulfilling legal obligations

Legal basis for data management: Legal obligation (GDPR Article 6 (1) point c)

Consent (Article 6(1)(a) GDPR)

Duration of data management: The personal data provided will be processed for the duration of the contractual relationship with the data subject, with the exception of: data to be kept for 8 years based on Act C of 2000 on accounting, and CL. 2017 on taxation. data to be kept by law until the last day of the 5th year following the relevant year.

Data is transferred to the NTAK system.

Upon arrival at the Hotel, before occupying the reserved room, the Data Subject fills out a hotel registration form, in which he consents to the Data Controller processing the data provided below for the purpose of fulfilling his obligations defined in the relevant legislation, and for the purpose of proving fulfillment, as well as for the identification of the Guest, as long as the competent authority you can check the fulfillment of obligations defined in specific legislation:

The activity and process involved in data management are as follows:

o The provision of mandatory data by the Guest is a condition for the use of hotel services.

o By signing the notification form, the guest consents to the fact that the data provided by filling out the notification form will be processed and archived by the Data Controller within the above-mentioned deadline for the purpose of proving the creation of the contract, the completion and fulfillment of the contract, and the possible assertion of claims.

5.4. Invoicing

The processed data are as follows: Last name*, First name*, Address*, Time of stay in the hotel*, Tax number in the case of a company*

Purpose of data management: Invoicing the use of hotel services, fulfilling invoicing obligations, conducting payment transactions

Legal basis for data management: Legitimate interest (GDPR Article 6(1)(f));

Fulfillment of a legal obligation (GDPR Article 6 (1) point c)

Duration of data management: data to be kept for 8 years based on Act C of 2000 on accounting, as well as CL of 2017 on taxation. data to be kept by law until the last day of the 5th year following the relevant year

Data will be forwarded to LAKI Zrt (1151 Budapest, Mogyoród útja 12-14.) for accounting purposes.

The Data Controller uses and may use the bank, credit card/bank account data provided to the Data Controller by the data subject only to the extent and for as long as it is necessary to exercise its rights and fulfill its obligations. The data are managed by the contractual banking partners of the Data Controller. You can find information about this data management on the websites of the relevant Bank.

5.5. Facebook page / Instagram page

The processed data are as follows: Photo recording, Facebook/Instagram ID, the name entered there

Purpose of data management: Utilizing the possibilities of the social site in order to promote the Hotel

Legal basis for data management: Consent (GDPR Article 6 (1) point a)

Duration of data management: Until consent is revoked, until the day of unsubscription

No data transmission takes place.

* By clicking on the "like" link on the Data Manager's Facebook/Instagram page, the data subject consents to the publication of the Data Manager's news and offers on his own message wall.

* Data controller also publishes pictures/films about various events/hotels/fitness clubs/restaurants etc. on his Facebook/Instagram page. If it is not a mass recording, the Data Controller always asks for the written consent of the data subject before publishing the images..

* You can get information about the data management of the Facebook/Instagram site from the data protection guidelines and regulations on the Facebook/Instagram website at www.facebook.com, www.instagram.com

5.6. Guest book

The processed data are as follows: Data subject name*, Data subject opinion*

Purpose of data management: Managing the guest book on the vinumhotel.hu website.

Legal basis for data management: Consent (GDPR Article 6 (1) point a)

Duration of data management: Until withdrawal of consent.

No data transmission takes place.

* In order to improve the quality of the service, the data subjects can submit their opinions online.

* Providing the data is not mandatory, it only serves to accurately investigate possible complaints and to ensure that the Data Controller responds to the guest.

* The Data Controller may also use the opinions received in this way, as well as any related data that cannot be traced back to the given Guest or linked to the Guest's name, for statistical purposes.

* The Data Controller stores the provided personal data in a separate data file, separately from other provided data. This data file can only be accessed by authorized employees of the Data Controller.

5.8. Electronic monitoring system

The processed data are as follows: Image

Purpose of data management: Personal and property security

Legal basis for data management: Consent (GDPR Article 6 (1) point a)

Duration of data management: maximum 2 weeks

No data transmission takes place.

The recorded images are forwarded if, based on the recordings, it seems probable that a crime (violation) has been committed, in which case the recordings may be forwarded to the investigative authority, or if other legal proceedings need to be initiated based on the recordings, in which case the recordings will be sent to the competent authority are forwarded to a court or authority.

* Cameras operate in the Hotel area operated by the Data Controller for the safety of the guests' lives, physical health and property, informational signs call the attention of those concerned to their operation. Regarding the legal operation of the surveillance system, the Data Controller acts in accordance with the provisions made in this information sheet and the camera regulations and makes them available to those concerned.

* Special rules for the operation of the camera surveillance system:

o In accordance with the provisions of this information, the camera surveillance system is governed by a separate regulation, the current version of which is available at the Hotel's reception.

o The camera system records an image.

o The purpose of data management: personal and property security..

o The place where the recording is stored: the hotel operated by the Data Controller, located at 8230 Balatonfüred Táncsics Mihály utca 7.

o The legal basis for data management: the voluntary consent of the data subject based on the Operator's information posted in the form of signs. Consent can also be given in the form of suggestive behavior. Suggestive behavior, especially if the person concerned enters or stays in the units affected by the camera surveillance system.

o The Operator must ensure that the personal data of the person concerned, especially his private secrets and the circumstances of his private life, are protected from unauthorized access.

o Electronic monitoring systems cannot be used in places where monitoring may violate human dignity, such as especially in changing rooms, showers and washrooms, toilets, and rest areas. Camera surveillance is proportionate to its purpose, the Data Controller does not conduct unlimited and direct surveillance.

o Storage duration of the recording: If the recorded image is not used, it must be destroyed or deleted no later than 3 days after recording. Use is defined as if the recorded image and other personal data are used as evidence in court or other official proceedings.o The person whose right or legitimate interest is affected by the recording of the image or other personal data, within 3 days of its recording, by proving his right or legitimate interest you can request that the data is not destroyed or deleted by its manager.

Upon request of a court or other authority, the recorded recording and other personal data must be sent to the court or authority immediately. If an inquiry is not made within thirty days of the request not to destroy it, the recorded image and

other personal data must be destroyed or deleted, unless the camera surveillance system has not yet expired.

6. Website visit data (References and links)

6.1. he Data Controller's website may also contain links that are not operated by the Data Controller and are only for the information of visitors. The Data Controller has no influence on the content and security of the websites operated by the partner companies, so it is not responsible for them.

6.2. Please review the data management regulations and data protection declarations of the pages you visit before entering your data in any form on that page.

6.3. Analytics, cookies

1. The Data Controller uses an analytical tool to monitor its websites, which creates a series of data and monitors how visitors use the Internet pages. The system creates a cookie when viewing the page, with the aim of recording information related to the visit (visited pages, time spent on our pages, browsing data, exits, etc.), but this is data that cannot be associated with the person of the visitor. This tool helps to improve the ergonomics of the website, to create a user-friendly website, in order to enhance the online experience of the visitors. The Data Controller does not use analytical systems to collect personal information. Most Internet browsers automatically accept cookies, but visitors have the option to delete them or refuse them automatically. Since every browser is different, the visitor can set their cookie preferences individually using the browser toolbar. You may not be able to use certain features on our website if you choose not to accept cookies.

2. On the website, we use a session cookie (a small data package), which is valid until the end of the given session, i.e. it is created for the duration of the visit, after which it is automatically deleted from the user's computer. The so-called cookie is necessary for the security of the website, for user-friendly solutions, for a better user experience.

7. STORAGE OF PERSONAL DATA, INFORMATION SECURITY

7.1. Personal data can only be handled in accordance with the activities according to Chapter 5, according to the purpose of data management.

7.2. It is possible to modify and delete personal data, withdraw voluntary consent, and request information about the handling of personal data by sending a notification to info@petitbois.hu.

7.3. The Data Controller ensures the security of the data. To this end, it takes the necessary technical and organizational measures, develops procedural rules and enforces them.

7.4. The Data Manager protects the data with appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage, as well as against becoming

inaccessible due to changes in the technology used. The data manager takes all necessary technical and organizational measures to avoid a possible data protection incident (e.g. damage, disappearance of files containing personal data, access to unauthorized persons). In the event of an incident that does occur, the data controller keeps a record for the purpose of checking the necessary measures and informing the data subject, which includes the range of personal data concerned, the range and number of persons affected by the data protection incident, the date, circumstances, effects of the data protection incident and the measures taken to prevent it, and other data specified in the law that prescribes data management.

7.5. In order to enforce the conditions of data security, the Data Controller ensures the appropriate preparation of the Employees concerned.

7.6. When determining and applying measures for data security, the Data Controller takes into account the state of the art at all times and chooses from several possible data management solutions the one that ensures a higher level of protection of personal data, unless it would represent a disproportionate difficulty.

7.7. As part of its duties related to IT protection, the Data Controller ensures in particular:

1. On the measures ensuring protection against unauthorized access, including the protection of software and hardware devices, and physical protection (access protection, network protection);

2. About the measures that ensure the possibility of restoring data files, including regular backups and separate, safe handling of copies (mirroring, backups);

3. On the protection of data files against viruses (virus protection);

4. About the physical protection of the data files and the devices carrying them, including protection against fire damage, water damage, lightning strikes, and other elemental damage, as well as the reparability of damage caused by such events (archiving, fire protection).

7.8. The Data Controller provides the required level of protection during the processing of the data - especially their storage, correction, deletion - when requesting information or objecting to the data subject.

7.9. Data transmission takes place with the consent of the data subject, without prejudice to his interests, confidentially, with the provision of a fully adequate IT system, and in compliance with the purpose, legal basis and principles of data management. The Data Controller will not forward the data subject's personal data or make them available to third parties without their consent, unless this is required by law.

7.10. The other data concerned, which cannot be linked directly or indirectly, and cannot be identified - hereafter anonymous - are not considered personal data.

8. EXERCISE OF THE RIGHTS OF THE SUBJECT

8.1. Your rights are affected

The data subject may request information from the Data Controller about the management of his personal data, as well as request the correction, deletion, or withdrawal of his personal data, limitation of data processing, and may exercise his right to data portability and objection.

a.) Right to information:

At the request of the data subject, the Data Controller shall take appropriate measures in order to provide data subjects with all the information and information specified in the General Protection Regulation regarding the handling of personal data in a concise, transparent, understandable and easily accessible form, clearly and comprehensibly worded.

b.) The data subject's right to access: The data subject is entitled to receive feedback from the Data Controller as to whether his personal data is being processed, and if so, he is entitled to access the personal data and the following information:

• the purposes of data management;

• categories of personal data concerned;

• recipients or categories of recipients to whom or to whom the personal data has been or will be communicated, including in particular recipients in third countries and international organizations;

• the planned period of storage of personal data; the right to rectification, deletion or limitation of data processing and the right to protest; the right to submit a complaint to the supervisory authority;

• information about data sources;

• the fact of automated decision-making, including profiling, as well as comprehensible information about the applied logic and the significance of such data management and the expected consequences for the data subject.

The Data Controller provides a copy of the personal data that is the subject of data management to the data subject. For additional copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs. At the request of the data subject, the Data Controller provides the information in electronic form.

The right to information can be exercised in writing via the contact details indicated in point 1. At the request of the person concerned, information can also be given orally after valid proof of identity and identification.

c.) Right to rectification:

The data subject may request the correction of inaccurate personal data concerning him/her managed by the Data Controller and the addition of incomplete data.

d.) Right to erasure:

If one of the following reasons exists, the data subject has the right to request that the Data Controller delete his/her personal data without undue delay:

• personal data are no longer needed for the purpose for which they were collected or otherwise processed;

• the data subject withdraws his consent, which is the basis of the data management, and there is no other legal basis for the data management;

• the data subject objects to data processing and there is no overriding legal reason for data processing;

• personal data were handled illegally;

• the personal data must be deleted in order to fulfill the legal obligation prescribed by the European Union or Member State law applicable to the Data Controller.

• the collection of personal data took place in connection with the offering of services related to the information society.

Data deletion cannot be initiated if data management is necessary:

• for the purpose of exercising the right to freedom of expression and information;

• for the purpose of fulfilling the obligation according to the European Union or national law applicable to the data controller, which prescribes the processing of personal data, or for the execution of a task carried out in the public interest or in the context of the exercise of public authority conferred on the data controller;

• in the field of public health, or for archival, scientific and historical research purposes or for statistical purposes, based on public interest;

• or to present, assert or defend legal claims.

e.) The right to restrict data processing:

At the request of the data subject, the Data Controller restricts data processing if one of the following conditions is met:

• the data subject disputes the accuracy of the personal data, in which case the restriction applies to the period that allows the accuracy of the personal data to be checked;

• the data management is illegal and the data subject opposes the deletion of the data and instead requests the restriction of their use;

• the Data Controller no longer needs the personal data for the purpose of data management, but the data subject requires them to submit, enforce or defend legal claims; or

• the data subject objected to data processing; in this case, the restriction applies to the period until it is determined whether the Data Controller's legitimate reasons take precedence over the data subject's legitimate reasons. If data management is subject to restrictions, personal data may only be processed with the consent of the data subject, with the exception of storage, or to submit, enforce or defend legal claims, or to protect the rights of another natural or legal person, or in the important public interest of the European Union or a member state. The Data Controller informs the data subject in advance of the lifting of restrictions on data management.

f.) Right to data portability:

The data subject has the right to receive the personal data concerning him/her provided to the Data Controller in a segmented, widely used, machine-readable format, and to forward this data to another data controller.

g.) Right to protest:

The data subject has the right to object at any time for reasons related to his own situation to the processing of his personal data necessary for the performance of tasks carried out in the public interest or in the context of the exercise of public authority granted to the data controller, or the processing necessary to assert the legitimate interests of the Data Controller or a third party.

In the event of a protest, the Data Controller may no longer process the personal data, unless it is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or that are related to the submission, enforcement or defense of legal claims.

In order to obtain direct business, the Data Controller does not process personal data.

8.2. Procedural rules

The Data Controller shall inform the data subject of the measures taken following the request without undue delay, but in any case within one month of the receipt of the request. If necessary, taking into account the complexity of the application and the number of applications, this deadline can be extended by another two months. The Data Controller shall inform the data subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request. If the data subject submitted the request electronically, the information will be provided electronically, unless the data subject requests otherwise.

If the Data Controller does not take measures following the data subject's request, it shall inform the data subject without delay, but at the latest within one month of the receipt of the request, of the reasons for the failure to take action, and of the fact that the data subject may file a complaint with a supervisory authority and exercise his right to judicial redress.

The Data Controller provides the requested information and information free of charge. If the data subject's request is clearly unfounded or - especially due to its repeated nature - excessive, the Data Controller may, taking into account the administrative costs associated with providing the requested information or information or taking the requested measure, charge a reasonable fee or refuse to take action based on the request.

The Data Controller informs all recipients of all corrections, deletions or data management restrictions carried out by them, to whom or to whom the personal data was communicated, unless this proves to be impossible or requires a disproportionately large effort. At the request of the data subject, the Data Controller informs about these recipients.

The Data Controller provides a copy of the personal data that is the subject of data management to the data subject. For additional copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. If

the data subject submitted the request electronically, the information will be provided in electronic format, unless the data subject requests otherwise.

8.3. Compensation and damages

All persons who have suffered material or non-material damage as a result of a violation of the General Protection Regulation are entitled to compensation from the Data Controller or data processor for the damage suffered. The Data Processor is only liable for damages caused by data processing if it has not complied with the obligations specifically imposed on data processors as defined by law, or if it has ignored or acted contrary to the lawful instructions of the Data Controller. If both the Data Controller and the data processor are involved in the same data processing and are liable for the damages caused by the data processing, the Data Controller and the data processor are jointly responsible for the entire damage. The Data Controller or the data processor is exempted from liability if it proves that it is not in any way responsible for the event causing the damage.

8.4. Data protection official procedure

The data subject may submit a complaint regarding the handling of his personal data by the Data Controller to the National Data Protection and Freedom of Information Authority, as a supervisory authority. Contact details of the supervisory authority National Data Protection and Freedom of Information Authority (NAIH)

address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

postal address: 1530 Budapest, Pf.: 5.

e-mail: ugyfelszolgalat@naih.hu

telephone: +36 (1) 391-1400

fax: +36 (1) 391-1410

In the case of violation of the rights of a deceased person with offensive, hateful, or exclusionary content, rectification, or violation of the rights of a deceased person, you can file a report or complaint:

National Media and Communications Authority

address 1015 Budapest, Ostrom u. 23-25.

e-mail: info@nmhh.hu

mailing address: 1525. Pf. 75

phone: (06 1) 457 7100

fax: (06 1) 356 5520

9. DATA PROTECTION INCIDENT REPORTING SYSTEM

9.1. Data protection incident: a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise handled.

9.2. Notification of the data protection incident to the supervisory authority

1. The Data Controller shall report the data protection incident to the competent supervisory authority without undue delay and, if possible, no later than 72 hours after becoming aware of the data protection incident, unless the data protection incident is likely to pose no risk to the rights and freedoms of natural persons looking at. If the notification is not made within 72 hours, the reasons justifying the delay must also be attached.

2. The Data Processor shall report the data protection incident to the data controller without undue delay upon becoming aware of it. (24 hours maximum)

3. If and to the extent that it is not possible to provide the information at the same time, it can be provided later in parts without further undue delay.

4. The Data Controller keeps records of data protection incidents, indicating the facts related to the data protection incident, its effects and the measures taken to remedy it.

9.3. Informing the data subject about the data protection incident

1. If the data protection incident likely entails a high risk for the rights and freedoms of natural persons, the data controller shall inform the data subject of the data protection incident without undue delay (maximum 24 hours).

2. In the information provided to the affected party, the nature of the data protection incident must be clearly and comprehensibly described, and the above-mentioned information and measures must be communicated.

3. The data subject does not need to be informed if any of the following conditions are met:

* the Data Controller has implemented appropriate technical and organizational protection measures and these measures have been applied to the data affected by the data protection incident, in particular those measures - such as the use of encryption - that make them unintelligible to persons not authorized to access personal data the data;

* after the data protection incident, the Data Controller took additional measures to ensure that the high risk to the rights and freedoms of the data subject mentioned in the previous paragraph is unlikely to materialize in the future;

* providing information would require a disproportionate effort. In such cases, the data subjects must be informed through publicly published information, or a similar measure must be taken,

which ensures equally effective information to the stakeholders.

Date: November 1, 2024

Péter Laki

managing director Petit Bois Kft.

Data marked with * must be filled in.