

Melea

THE HEALTH CONCEPT



UNIONE SÁRVÁR

Szállodaprojekt

Korlátolt Felelősségű Társaság

**PUBLIC DATA
PROCESSING NOTICE**



Public Data Processing Notice of UNIONE Sárvár Kft.

Please take the time to carefully read this information document to understand how we handle your personal data. If you have any questions, please do not hesitate to contact us using the provided contact information. Feel free to reach out to us with any questions!

The Service Provider operates a premium category recreation center and hotel called "MELEA THE HEALTH CONCEPT HOTEL" at 9600 Sárvár, Rákóczi Ferenc Street 28, in the framework of which the Service Provider processes the personal data of hotel guests and patients using its various services, as well as visitors to its website. UNIONE Sárvár Ltd. as a data controller respects the privacy of all persons who provide personal data and does everything in its power to protect them.

This notice applies equally to our clients, employees working for our clients, website visitors, hotel guests, partners, suppliers (and potential suppliers), and their employees.

During its operation, UNIONE Sárvár Kft. uses the assistance of external partners to perform certain tasks. During the performance of these tasks, it has contractual relationships with partners, which contracts cover the rules of data processing. It has joint data controller or data processor relationships with these partners, for whom the guidelines of this data protection policy are equally applicable.

Please read our notice carefully to understand how we handle your personal data. If you have any questions, do not hesitate to contact us using our provided contact details. We are happy to assist you!

I./ Data Controller Information

Name: UNIONE SÁRVÁR Szállodaprojekt Korlátolt Felelősségű Társaság
Registered office: 1123 Budapest Alkotás u. 55-61.
Site: 9600 Sárvár Rákóczi u. 28.
Registration no.: 01-09-068756
Phone: +36 95 523 900
Email: info@melea.hu

Data Protection Officer Information:

Name: Horváth Réka
Address: 1123 Budapest, Alkotás u. 55-61.
Email: dpo@melea.hu

Feel free to contact us with any data protection issues.

II./ Principles of Data Processing

- II./1. Lawfulness, fairness, and transparency
- II./2. Necessity and proportionality
- II./3. Purpose limitation
- II./4. Data minimization
- II./5. Accuracy
- II./6. Storage limitation
- II./7. Integrity and confidentiality
- II./8. Accountability



III./1. A Lawfulness, fairness, and transparency

Personal data must be processed lawfully, fairly, and in a transparent manner for you.

During the processing of personal data, it is important that every step is lawful, happens in a fair manner, and is completely transparent for the data subjects (such as you).

- **Lawfulness and Fairness:** This means that data must be obtained through legal and honest means, and these principles must remain valid throughout the entire data processing period. Data processing must always rely on a legal basis, such as consent, contract performance, legal obligation, vital interest, public interest, or the legitimate interest of the data controller.
- **Transparency:** Data processing must always occur in a way that allows the data subjects (you) to know all the details about the processing of their data. For example, you need to know what data we collect,

why, how long we store it, and to whom we might transfer it (such as to an accountant or other data controller). Transparency ensures that you can effectively exercise your rights and receive all the information you need.

It is important to note that there are limitations to the obligation to inform, and it is not necessarily required to notify every data subject personally. Providing information through a notice on a website may also meet the requirements. However, in certain cases (such as significant changes in data processing), we may be obligated to notify you by email.

The GDPR stipulates that if someone else provides us with your data (we do not receive it from you), we must notify you as soon as possible, but no later than within one month.

III./2. Necessity and proportionality

When processing your data, we always fully comply with the principle of necessity and proportionality. Necessity means that the data processing is absolutely necessary to achieve the data processing purpose. Proportionality sets the framework for this necessity by requiring that the limitation of fundamental rights and freedoms necessary for data processing must also be proportionate to the objective.

The Constitution states that a fundamental right may be restricted in order to enforce another fundamental right or to protect a constitutional value, to the extent absolutely necessary, proportionate to the objective to be achieved, with respect for the essential content of the fundamental right.

III./3. Purpose limitation

Data collection must always be for clear and lawful purposes, and these purposes cannot be mixed. So before any data collection, we precisely determine what the data will be used for, and we only serve that purpose. Data processing can never go against the law.

However, there are cases when we can process the same data for multiple purposes. For example, if we first collect your name for a quote request, later, when you become our guest, we can use it for order fulfillment, and then for invoicing. In these cases, the data processing purposes are different and well-separated from each other.

We can use the data for multiple purposes simultaneously. For example, after fulfilling a contract, we may keep them for legitimate interest, such as evidence in a potential legal dispute. At the same time, we may process the same data for other reasons, such as the obligation to issue invoices.



If the data processing purposes change, we will always send you information about this.

It is important to note that under the GDPR, certain cases are not considered incompatible with the original purpose, for example, data processing for public archiving purposes, scientific research, or statistical analysis.

III/4. Data minimization

We store personal data in a manner that is appropriate and relevant to the purposes of data processing and limit it to what is necessary. We do not process data that is not needed to achieve the purpose.

III/5. Accuracy

We always store your personal data accurately and up-to-date to the best of our knowledge. If it turns out that the data is inaccurate or outdated in relation to the purpose of processing, we take all reasonable steps to correct it. However, it's important to note that excessive expectations are not realistic. We cannot be expected to check every day if someone's name is still the same. However, if we become aware that your data has changed or was incorrectly provided to us, and this does not conflict with the purpose of data processing, we will correct it. Please notify us if such changes have occurred in your data.

Maintaining the accuracy of data is one of our primary duties, but if you notice any inaccuracies, please let us know so we can correct them.

III/6. Storage limitation

Personal data is stored in a form that allows your identification only for as long as necessary for the purposes of processing personal data. After this, we delete the data. Our IT system has been designed so that electronically stored data is deleted by the deadline. The exact time of data storage and the rules for data disposal are regulated in our data processing policy, and we always act accordingly. We do not store data unnecessarily.

Your personal data will only be stored for longer than the above if the processing of personal data is carried out in accordance with the GDPR for purposes of public archiving, scientific and historical research, or statistical purposes, also taking into account the implementation of appropriate technical and organizational measures prescribed in the GDPR for the protection of your rights and freedoms.

III/7. Integrity and confidentiality

When processing your personal data, we strive to apply appropriate technical and organizational measures that ensure the security of the data. This means we protect data from unauthorized or unlawful processing, accidental loss, destruction, or damage. We have designed our data storage system in such a way that even within the company, access to data is restricted to prevent unauthorized use. For example, if an employee is not involved in processing bookings made on the website, we have ensured through permission settings that they cannot access this data.

III/8. Accountability

UNIONE Sárvár Kft. is responsible for compliance with data protection regulations and is able to demonstrate this compliance. In Hungary, the primary authority is the National Authority for Data Protection and Freedom of Information, or NAIH for short.

In case of a report (or sometimes officially initiated), NAIH examines whether a company's data processing is lawful and fully complies with legal requirements. During such an investigation, the data controller must be able to prove and demonstrate that their data processing complies with regulations. An important part of this is having a data protection policy in which data processing is lawfully regulated.



UNIONE Sárvár Kft. has developed a data processing and data security policy for its entire data processing operation and conducts its data processing accordingly.

III. Lawfulness of data processing

When designing our data processing, we always ensure that data processing complies with the principle of lawfulness. We conduct our data processing based on the following legal bases, taking into account the highlighted detailed rules.

- III/1. Consent of the data subject
- III/2. Performance of a contract
- III/3. Legal obligation
- III/4. Vital interest
- III/5. Public interest or exercise of official authority
- III/6. Legitimate interest

III/1. Consent of the data subject

You have given consent to the processing of your personal data for one or more specific purposes. It is important that consent is voluntary and that you provide consent through an active action in each case.

III/2. Performance of a contract

The processing is necessary for the performance of a contract to which you are a party, or the processing is necessary for taking steps at your request prior to entering into a contract.

III/3. Legal obligation

The processing is necessary for compliance with a legal obligation to which we are subject. We only process data on the legal basis of a legal obligation if there is a statutory requirement. We do not apply legal obligation as a legal basis for data processing when a law prescribes data processing in a conditional manner.

III/4. Vital interest

The processing is necessary to protect your vital interests or those of another natural person. An important consideration in selecting this legal basis is that data processing based on vital interest is temporary in nature and may only last for the duration of the vital interest. We separately regulate the management of data after the vital interest ceases.

III/5. Public interest or exercise of official authority

In this case, the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us. We are not considered a public authority and do not perform data processing in the public interest, so we currently do not process data on this basis.

III/6. Legitimate interest

The processing is necessary for the purposes of the legitimate interests pursued by UNIONE Sárvár Kft. or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data, especially if you are a child. We often process data on this basis during our data processing.

In the case of data processing based on legitimate interest, we have always carried out a balancing test, in which we examined the proportionality and necessity of the impact and limitation on your fundamental rights and freedoms.



IV. Data security

UNIONE Sárvár Kft. is committed to protecting personal data against loss, unlawful use, unlawful transfer, modification, unavailability, or destruction, and takes all necessary measures to preserve the confidentiality of personal data, including the use of appropriate technical and organizational measures.

Organizational measures include controlling physical access to our buildings, training employees, and storing paper-based files in appropriate rooms. Technical measures include encryption related to access to our systems, password protection, and the use of antivirus software.

As part of the process by which you provide us with your personal data, this data may also be transmitted over the internet. Despite taking all necessary measures to protect the personal data you provide to us, data transmission over the internet cannot be considered completely secure. Accordingly, you must acknowledge and accept that we cannot take full responsibility for the security of data transmission through our website, and such transmission may be at your own risk. However, once your personal data arrives in our systems, we follow strict procedures for security and to prevent unlawful access.

In cases where we have given you a password (or you have chosen one), you are responsible for maintaining the confidentiality of this password. We ask that you do not share this password with anyone.

Our websites or social media pages may from time to time contain references to websites operated by third parties, including websites of member companies and partner networks; the new data processing of these does not fall within the scope of our activities.

V. Cookies management

V/1. What is a cookie?

V/2. Why do we use cookies?

V/3. What kinds of cookies do we use?

V/4. Cookie settings

V/5. Data protection information related to essential cookies

V/1. What is a cookie?

A cookie is a small text file that is placed on your computer when you visit a website. Cookies have multiple functions, including collecting information, remembering user settings, and allowing the website owner to understand user habits to enhance the user experience. You can manage your cookie settings in your browser settings at any time.

V/2. Why do we use cookies?

- We use cookies to develop our pages,
- To enhance user experience,
- To facilitate the management of our pages,
- To gather information about user habits,
- To place targeted advertisements.

V/3. What kinds of cookies do we use?

Essential cookies for site operation

Essential cookies help make our website usable by enabling basic functions such as page navigation and access to secure areas of the website. The website cannot function properly without these cookies.



Preference cookies

Preference cookies allow us to remember information that changes the behavior or appearance of the website, such as your preferred language or the region where you are located.

Statistical cookies

Through anonymous collection and reporting of data, statistical cookies help the website owner understand how visitors interact with the website.

Marketing cookies

Marketing cookies are used to track visitors across websites. The aim is to display advertisements that are relevant and engaging for individual users and thereby more valuable for publishers and third-party advertisers.

The purpose of these cookies is to create user groups to display relevant advertisements and content. This process involves manual intervention.

These cookies are stored on your machine by the system. Cookies are not capable of identifying individuals.

We use remarketing services, such as Google AdWords remarketing, to deliver personalized advertisements to you. You can disable these cookies in the [Google Ad Settings Manager](#) according to the instructions provided there. You can learn about Google's advertising privacy policies by clicking [here](#).

V/4. Cookie settings

By default, all browsers allow the use of cookies. If you want to delete cookies from our pages or do not want to use them, please refer to the links below depending on which browser you use:

- [Google Chrome](#)
- [Edge](#)
- [Firefox](#)
- [Microsoft Internet Explorer 11](#)
- [Microsoft Internet Explorer 10](#)
- [Microsoft Internet Explorer 9](#)
- [Microsoft Internet Explorer 8](#)
- [Safari](#)

Please note that **if cookies are disabled**, certain elements or **the full functionality of the website may not be available**.

V/5. Data processing information related to cookies

Purpose of data processing

Essential cookies for site operation: ensuring the proper functioning of the website.

Our website development, facilitating your navigation on our website and during the use of the site's functions, thus ensuring a smooth user experience, collecting information about the use of our website, placing targeted advertisements on other websites (remarketing), tracking activities performed on the website so that we can deliver specifically interesting, relevant offers to you, delivering personalized offers to the contact details provided during registration.

Legal basis for data processing



For cookies essential for website operation:

The legal basis for data processing is Article 6(1)(f) of the GDPR, "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party"

For other cookies:

Consent of the data subject – GDPR Article 6(1) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

Presentation of legitimate interest

Without cookies, the website cannot fully function in all its features, and thus the website cannot achieve its purpose. On the other hand, the website needs to be protected from possible attacks. Therefore, the data controller has a compelling legitimate interest to record the online identifiers of users visiting the website that qualify as personal data (IP address), as well as other personal data generated in connection with browsing (time of browsing, browser type, some characteristics of the operating system used for browsing; such as operating system type and language settings), and thus prevent external attacks on the website and public electronic services. For all these reasons, the website operator data controller has a legitimate interest in using cookies that are essential for operation.

Categories of data subjects

Natural persons visiting the website

Categories of personal data

The online identifier of users visiting the website that qualifies as personal data (IP address), as well as other personal data generated in connection with browsing (time of browsing, browser type, some characteristics of the operating system used for browsing; such as operating system type and language settings).

The name of the cookie, the service provider, the purpose of the cookie, its type, and the duration of data processing for this purpose:

You can get more detailed, current information about these by clicking on cookie information at the bottom of the website.

Is it mandatory to provide personal data, consequences of failure to provide data

For cookies essential for website operation: Yes

Without this, you cannot access the site, and it cannot be used properly.

Enabling other cookies is not mandatory

Information about the fact of automated decision-making

An automated decision-making procedure is expected to be implemented by the data controller for data processing for this purpose.



VI. Individual data processing operations

During our data protection audit, we found that we perform data processing in the following cases:

- VI/1. Processing data of information requesters, service inquirers, price quote requesters (via email online, postal mail, telephone, in person)
- VI/2. Data processing related to contract fulfillment
- VI/3. Data processing for Medical, Recreational, and health maintenance treatments and services
- VI/4. Data processing for SMS and telephone notifications
- VI/5. Billing and other accounting data processing
- VI/6. Complaint data processing
- VI/7. Processing job applicants' data
- VI/8. Dormant data processing (during limitation period)
- VI/9. Data processing of camera recordings in the hotel area
- VI/10. Data processing related to the NTAK system
- VI/11. Data processing related to newsletters and marketing communications
- VI/12. Data processing related to bookings (through email and web systems)
- VI/13. Data processing related to check-in
- VI/14. Use of supplementary services
- VI/15. Personal data processing related to satisfaction measurement
- VI/16. Data processing related to social media platform usage
- VI/17. Data processing related to the operation of internal whistleblowing systems

VI/1. Processing data of information requesters, service inquirers, price quote requesters (via email online, postal mail, telephone, in person)

Purpose of data processing:

Answering potential customers' questions related to contract fulfillment, providing price quotes as preparation for a future contract

Legal basis for data processing:

Article 6(1)(b) second clause of the GDPR: "processing is necessary in order to take steps at the request of the data subject prior to entering into a contract"

Categories of data subjects:

Information requesters, product and service inquirers, price quote requesters

Categories of personal data:

Name, email address, phone number

Duration of data processing for this purpose:

Until withdrawal by the data subject.

Melea

THE HEALTH CONCEPT



In case of product availability, at the time it becomes available

In case of information request, until the response is provided

In case of providing a price quote, until the quote is accepted or rejected, or until the quote's validity period expires

Is it mandatory to provide your personal data, consequences of failure to provide data:

Not mandatory.

Without a name, we cannot address you.

Without an email address, we cannot notify you by email about product arrival

Without an email address, we cannot send you a price quote

Without a phone number, we cannot call you back and coordinate personally

Recipients of personal data:

Email service provider

Is there any data transfer to a third country or international organization

Data provided for this purpose is not transferred to a third country or international organization.

Information about automated decision-making:

No automated decision-making occurs during the processing of data provided for this purpose

VI/2. Data processing related to contract fulfillment

Purpose of data processing:

Contract conclusion and fulfillment of obligations undertaken in the contract, exercise of contractual rights.

Legal basis for data processing:

Contract performance - Article 6(2) of the GDPR "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

Categories of data subjects:

Natural person contracting parties

Categories of personal data:

Name, address, place and date of birth, mother's name, phone number, email address, other data specified in the contract

Duration of data processing for this purpose:

Until contract completion, in case of termination of contract performance for any reason, until contract termination

Is it mandatory to provide your personal data, consequences of failure to provide data:

Yes

Without the data, the contract cannot be established.



Recipients of personal data:

Accountant
Postal service, courier service
Email service provider, SMS service provider
Other performance assistants, subcontractors involved in fulfillment with prior notification

Is there any data transfer to a third country or international organization

Data provided for this purpose is not transferred to a third country or international organization.

Information about automated decision-making:

No automated decision-making occurs during the processing of data provided for this purpose

VI/3. Data processing for Medical, Recreational, and health maintenance treatments and services

Purpose of data processing:

Contract conclusion for medical, recreational, and health maintenance treatments and fulfillment of obligations undertaken in the contract. Processing data related to the performance of medical, recreational, and health maintenance treatments included in the service package.

Legal basis for data processing:

Contract performance - Article 6(2) of the GDPR "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

Processing of special categories of personal data during the preparation and performance of medical treatments is carried out for preventive medicine purposes and establishing medical diagnoses, providing health care, and fulfilling a contract with a healthcare professional.

The guarantee condition under Article 9(3) of the GDPR is ensured because medical activities are subject to confidentiality obligations regulated by Hungarian national law. The medical, recreational, and health maintenance treatments and services performed by the data controller are also carried out by a doctor or under a doctor's responsibility. Based on the above, it has been established that the data controller has an appropriate legal basis and guarantees for processing special categories of personal data for this purpose, and the necessary conditions exist.

Categories of personal data:

Name, address, place and date of birth, mother's name, phone number, email address, other data specified in the contract

In case of medical treatment: social security number

Other data provided for the treatment in advance and during the treatment, or otherwise coming to the data controller's knowledge, as well as data coming to knowledge during aftercare, among which there may be data concerning health status

Other data provided for the treatment in advance and during the treatment, or otherwise coming to the data controller's knowledge, as well as data coming to knowledge during aftercare, among which there may be data belonging to special categories of personal data such as laboratory results, measured and diagnosed health data, health data arising during treatment.



Duration of data processing for this purpose:

For recreational and health maintenance services: Until the end of the treatment - multiple sessions, according to the service package.

For medical treatments: Medical documentation is kept for 30 years from the date of data collection, and the final report for at least 50 years.

After the mandatory record-keeping period, for the purpose of medical treatment or scientific research - if justified - following prior notification - data may continue to be recorded. If further record keeping is not justified and the medical documentation has no scientific significance, the records must be destroyed.

If the medical documentation has scientific significance, it must be handed over to the competent archives after the mandatory record-keeping period, and the data controller will not continue to process the data in this case.

Is it mandatory to provide your personal data, consequences of failure to provide data

Yes, otherwise the treatment cannot be performed.

The provision of health and identification data by the data subject is voluntary, with a few exceptions for identification data required for accessing healthcare services.

Nevertheless, the patient's obligations are regulated by the Health Act, according to which:

The patient is obliged to respect the relevant legislation and the operational rules of the healthcare provider when using the healthcare service.

The patient - if their health condition allows - is obliged to cooperate with the healthcare professionals involved in their care according to their abilities and knowledge as follows:

- **inform them of everything necessary for diagnosing, preparing an appropriate treatment plan, and performing interventions,**
- **in particular about all previous illnesses, medical treatments, medication or therapeutic product use, health risk factors,**
- inform them - in connection with their own illness - about anything that may endanger the lives or physical integrity of others,
- in particular about infectious diseases and conditions and states that exclude the practice of an occupation,
- in case of infectious diseases specified in the decree of the minister responsible for healthcare, identify persons from whom they may have contracted the infectious disease or whom they may have infected,
- inform them of all previous legal declarations concerning healthcare, reliably verify their personal data required by law.

Recipients of personal data:

1. Data processing for public health, epidemiological, and occupational health purposes

The healthcare provider immediately forwards health and identification data that come to their knowledge during data collection to the health administration authority if they detect or suspect an infectious disease listed in Annex 1, Section A of the Health Data Act. ([click here to view these diseases](#))



The healthcare provider forwards the health and identification data of persons whose microbiological laboratory test results suggest or confirm the presence of infections, infectious diseases, poisonings, or their pathogens according to Annex 1, Section A. The healthcare provider also forwards test results for diseases specified in the ministerial decree among the infections, infectious diseases, poisonings listed in Annex 1, Section A that, contrary to previous probability, do not confirm the existence of the given disease.

2. Work-related data transfer obligation

The observing physician is obliged to immediately forward the employee's health and identification data to the occupational safety authority if

- they detect or suspect certain occupational diseases
- the person concerned during the practice of their occupation, in connection with it
- is exposed to chemical substances specified in a ministerial decree, and the concentration of the substance in their body exceeds the permitted level,
- as well as in case of noise, if hearing loss of 30 dB at 4000 Hz occurs in either ear.

3. Data transfer for public health purposes

If the affected patient (including the fetus) suffers from a congenital abnormality specified in a ministerial decree or a rare disease with an ORPHA code (hereinafter: rare disease), the physician detecting the abnormality or rare disease shall forward the person's identification and health data, and - in case of a minor - the name and address of their legal representative within 30 days from the detection of the abnormality or rare disease to the National Registry of Congenital Abnormalities in the manner specified in a ministerial decree.

Prior to this notification, the detecting physician checks whether the affected patient's data are already in the National Registry of Congenital Abnormalities. If the data have not yet been reported, the physician proceeds as above. If the check reveals that the patient's registered data are not complete, the reporting physician complements them.

4. Data transfer at the request or data request of an organization outside the healthcare network

Upon data request or written request from the following organizations, the treating physician and the health insurance agency shall transfer the health data of the person concerned and the identification data necessary for identification that the requesting or data requesting organization is authorized to process by law. The request or data request must indicate the health and identification data to be accessed, including data available based on the medical report taken by the healthcare provider. The requesting or data requesting organizations may be the following:

- in criminal cases, the court, prosecutor's office, investigating authority, preliminary procedure body, forensic expert; in civil litigation and non-litigation cases, as well as administrative cases, the administrative authority, prosecutor's office, court, forensic expert,
- bodies conducting minor offense proceedings,
- in the case of potential conscripts and conscripts, the district (metropolitan district) office of the metropolitan and county government office, the military administrative and central data processing body of the Hungarian Defence Forces, and the committee determining military health fitness,
- the national security services, for the purpose of performing tasks specified in Act CXXV of 1995 on National Security Services, within the authorization given therein,
- the military administrative and central data processing body of the Hungarian Defence Forces, for the purpose of wartime assignment of trained reserves during peacetime and the rapid and



differentiated call-up of trained reserves, within the scope specified in the Act on National Defence and the Hungarian Defence Forces,

- the chamber body with competence and jurisdiction to conduct ethical proceedings during ongoing ethical proceedings against a healthcare worker,
- the bodies performing internal crime prevention and crime detection tasks specified in the Act on the Police, as well as counter-terrorism bodies, for the purpose of performing tasks specified in the law, within the authorization given therein,
- the physician performing the post-mortem examination during a post-mortem examination,
- the transport safety body during professional investigations specified in the Act on the Professional Investigation of Air, Rail, and Water Transport Accidents and Other Transport Events, as well as in Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC.

When the data subject receives medical care for the first time, if the data subject has suffered an injury healing beyond 8 days and the injury is presumably the result of a crime, the treating physician immediately reports the data subject's identification data to the police.

When a minor data subject receives healthcare for the first time - also with regard to Section 17 of Act XXXI of 1997 on Child Protection and Guardianship Administration - the physician appointed by the healthcare provider providing the care is obliged to immediately notify the child welfare service competent for the location of the healthcare provider if

- it is presumed that the child's injury or illness is the result of abuse or neglect,
- they become aware of circumstances indicating abuse or neglect during the child's healthcare.

The consent of the data subject or the person otherwise authorized to dispose of the data is not required for the above data transfers.

5. Data transfer to the archives:

If the medical documentation has scientific significance, it must be handed over to the competent archives after the mandatory record-keeping period.

6. Mandatory data provision to the EESZT:

The EESZT is the Electronic Health Service Space.

UNIONE Sárvár Kft., as a connected data controller, is obliged to send the following documents created during healthcare through the EESZT to the operator for those authorized to access the medical documentation to access the relevant documents through the EESZT:

- outpatient record issued in outpatient specialist care,
- laboratory results,

7. Laboratory tests:

During the use of our hotel's health services, we request laboratory tests from blood samples for our guests.

8. Other recipients during data transfers

Postal service, courier service

Email service provider, SMS service provider

Other performance assistants, subcontractors involved in the performance with prior notification



Records of health and personal identification data

Health Data Act Section 28. § (1) Health and personal identification data collected about the data subject, necessary for medical treatment, as well as their transfer must be recorded. The record of data transfer must include the recipient, method, time of the transfer, and the scope of data transferred.

- The record-keeping tool can be any data storage device or method that ensures the protection of data according to Section 6.

Based on the above, the data controller maintains records of processed data using the **Netdoktor healthcare record software**.

- The treating physician prepares notes about the health data collected by themselves or other healthcare providers, as well as about their own related activities and measures. These notes form part of the records.

Is there any data transfer to third countries or international organizations

Data provided for this purpose are not transferred to third countries or international organizations.

Information about automated decision-making:

No automated decision-making occurs during the processing of data for this purpose.

VI/4. Data processing for SMS and telephone notifications

Purpose of data processing:

At your request, we will notify you by SMS and/or telephone about the appointments for treatments and services included in your service package before the treatment during your stay at the hotel. The purpose of sending reminders is to ensure you don't forget that you have a treatment scheduled for a specific time.

Legal basis for data processing:

GDPR Article 6 (2) "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

Categories of data subjects:

Data subjects with reservations

Categories of personal data:

Name, phone number and/or email address

Duration of data processing for this purpose:

Until withdrawal, but at most until the reservation date.

Is it mandatory to provide your personal data, consequences of failure to provide data:

No

If you do not provide your phone number, we cannot notify you by SMS.

Recipients of personal data:

SMS service provider



Is there any data transfer to third countries or international organizations

Data provided for this purpose are not transferred to third countries or international organizations.

Information about automated decision-making:

No automated decision-making occurs during the processing of data for this purpose.

VI/5. Billing and other accounting data processing

Purpose of data processing:

Preservation of billing data to fulfill obligations specified in the Accounting Act

Legal basis for data processing:

The data controller lawfully processes billing and other accounting data under GDPR as it is required by law.

Legal obligation - GDPR Article 6(1)(c): "processing is necessary for compliance with a legal obligation to which the controller is subject;"

Act C of 2000 on Accounting - Section 169 (1) - (6)

Categories of data subjects:

Customers, other participants in accounting processes (e.g., actual payers)

Categories of personal data:

Name, address, other data required by law or displayed at the customer's request.

Duration of data processing for this purpose:

As specified by law, generally for a period of 8 years.

Is it mandatory to provide your personal data, consequences of failure to provide data:

Mandatory,

Without providing data, we cannot fulfill our legal obligations

Recipients of personal data:

Accountant, supervisory authorities

Data processing: Our company's accounting is handled by an external partner under a contractual relationship. This contract also covers the rules of data processing. The accounting firm always processes the personal data of Data Subjects based on our assignment, exclusively according to the guidelines of this privacy policy, and is not authorized to transfer it to third parties. Name and address of accounting firm: ICT Europa Finance Zrt. 1117 Budapest, Fehérvári út 50-52.

Is there any data transfer to third countries or international organizations

Data provided for this purpose are not transferred to third countries or international organizations.

Information about automated decision-making:



No automated decision-making occurs during the processing of data for this purpose.

VI/6. Complaint data processing

Purpose of data processing:

Fulfillment of legal obligations arising from warranty and guarantee claims, and handling other complaints

Legal basis for data processing:

The data controller lawfully processes data under GDPR as it is required by law.

Legal obligation - GDPR Article 6(1)(c): "processing is necessary for compliance with a legal obligation to which the controller is subject;

Act C of 2000 on Accounting - Section 17/A. (7) "The company is obliged to keep the complaint record and a copy of the response for five years, and to present it to the supervisory authorities upon request."

The basic rules of defective performance are contained in Chapter XXIV of the Civil Code, but other laws may also provide for it

Categories of data subjects:

Persons making warranty and guarantee claims and other complaints

Categories of personal data:

Name, Address, based on legal obligation, according to Act CLV of 1997, Section 17/A. (5), the complaint record must include the following: a) consumer's name, address

Processing of other data required by law and provided by the complainant may also occur, about which the complainant will be informed in the complaint handling record.

Duration of data processing for this purpose:

As specified by law, generally for a period of 5 years.

Is it mandatory to provide your personal data, consequences of failure to provide data:

Mandatory,

Without providing data, we cannot address your complaint and cannot fulfill our legal obligations

Recipients of personal data:

Email service provider,

Mail and package delivery, courier service

Authorities and courts

Is there any data transfer to third countries or international organizations

Data provided for this purpose are not transferred to third countries or international organizations.

Information about automated decision-making:



No automated decision-making occurs during the processing of data for this purpose.

VI/7. Processing job applicants' data

Purpose of data processing:

Advertising job opportunities, filling vacant positions

Legal basis for data processing:

The data controller lawfully processes the necessary data in preparation for a future contract under GDPR.

GDPR Article 6(1)(b) second part: "processing is necessary in order to take steps at the request of the data subject prior to entering into a contract"

Categories of data subjects:

Job applicants

Categories of personal data:

Name, phone number, and email address for notifications
Necessary data according to the conditions specified in the job posting.
Other data voluntarily provided by the applicant beyond the requirements

Duration of data processing for this purpose:

Until the position is filled or the job application is closed, but for a maximum of 3 months; in case of withdrawal by the data subject, until withdrawal

Recipients of personal data:

Email service provider

Is it mandatory to provide your personal data, consequences of failure to provide data:

No

Without the minimum data requested in the job posting, we cannot evaluate the application; without contact information, we cannot notify you.

Providing voluntarily given data is not mandatory; its absence has no effect on the application.

Is there any data transfer to third countries or international organizations

Data provided for this purpose are not transferred to third countries or international organizations.

Information about automated decision-making:

No automated decision-making occurs during the processing of data for this purpose.

VI/8. Dormant data processing (during limitation periods)

Purpose of data processing:



Providing evidence during legal enforcement following contract performance in administrative and court proceedings

Legal basis for data processing:

The data controller has a legitimate interest in data processing following contract performance, which is lawful

Legitimate interest - GDPR Article 6(1)(f): "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party,"

Processing of special categories of personal data is lawful under GDPR Article 9(2)(f) if processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity;

Demonstration of legitimate interest

The data controller has a legitimate interest in being able to reconstruct events during an administrative or court proceeding and have adequate evidence. Following the determination of legitimate interest, we conducted a balancing test, based on which the data processing is lawful.

We conducted a balancing test regarding legitimate interest, based on which we determined that UNIONE Sárvár Kft.'s legitimate interest does not disproportionately restrict the data subject's right to data protection.

Categories of data subjects:

Individual contracting parties, representatives of non-individual contracting parties, their authorized representatives, contact persons

Categories of personal data:

Name, Address, Place and date of birth, Mother's name, Email, Phone number, Mailing address, Other data provided for performance and necessary for claim enforcement, which may also contain special health data

Duration of data processing for this purpose:

Until the expiration of the limitation period, generally for 5 years.

According to Civil Code Section 6:22 (1), 5 years following the performance of the contract or termination of the contract without performance for any reason, or until another limitation period if prescribed by law. Other data that comes into our possession will only be retained if it may be relevant to the merits of the case or for later proof of actions.

Is it mandatory to provide personal data, consequences of failure to provide data:

Yes

Without providing the data, we cannot enter into a contract.

Recipients of personal data:

Email service provider:

Authorities and courts

Legal representative

Is there data transfer to a third country or international organization

We do not transfer data provided for this purpose to a third country or international organization.



Information about automated decision-making:

No automated decision-making occurs in the processing of data for this purpose

VI/9. Data processing of camera recordings in the hotel area

Purpose of data processing:

To secure the premises of Melea The Health Concept Hotel operated by UNIONE Sárvár Kft., for the purpose of life, physical integrity, and property protection

Legal basis for data processing:

The data controller has a legitimate interest in using cameras, which is lawful.

Legitimate interest - GDPR Article 6(1)(f) "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party,"

Demonstration of legitimate interest

UNIONE Sárvár Kft. uses the camera surveillance system in the hotel premises for the protection of human life, physical integrity, and property.

Categories of data subjects:

Persons entering the hotel premises and employees

Categories of personal data:

Image of the data subjects

Duration of data processing for this purpose:

We store the recordings for 15 working days, after which they are deleted. If the hotel remains closed for more than 15 working days, the retention period lasts until the end of the working day following reopening.

Is it mandatory to provide personal data, consequences of failure to provide data:

Yes

Without providing the data, you cannot visit our hotel.

Recipients of personal data:

Authorities, court

Is there data transfer to a third country or international organization

We do not transfer data provided for this purpose to a third country or international organization.

Information about automated decision-making:

No automated decision-making occurs in the processing of data for this purpose

VI/10. Data processing related to the NTAK system

Purpose of data processing:



During the operation of Melea The Health Concept Hotel, in compliance with its legal obligations, it provides statistical data through the NTAK system in accordance with the provisions of Act CLVI of 2016 on state tasks for the development of tourism areas and Government Decree 235/2019. (X. 15.) on state tasks for the development of tourism areas.

Legal basis for data processing:

The data controller lawfully processes data under GDPR as it has a legal obligation to do so.

Legal obligation - GDPR Article 6(1)(c): "processing is necessary for compliance with a legal obligation to which the controller is subject;"

Categories of data subjects:

Guests

Categories of personal data:

- the family name and first name of the person using accommodation services, birth family name and first name, place and date of birth, gender, nationality, and mother's birth family name and first name,
- identification data of the identification document or travel document of the person using accommodation services, in case of third-country nationals, the visa or residence permit number, date and place of entry, and
- the address of the accommodation service, the start and expected, as well as actual end date of the accommodation use.

Is it mandatory to provide personal data, consequences of failure to provide data:

The person using accommodation services must present their identification document to the accommodation provider for the purpose of recording the data. If the document is not presented, the accommodation provider will refuse to provide the accommodation service.

Data processor:

Magyar Turizmus Ügynökség Zrt.

Is there data transfer to a third country or international organization

We do not transfer data provided for this purpose to a third country or international organization.

Information about automated decision-making:

No automated decision-making occurs in the processing of data for this purpose

VI/11. Data processing related to newsletters and marketing communications

Our hotel is a member of the Unione Group, which enables our guests to receive an even more complete and personalized experience. In line with this, certain tasks - especially the organization of marketing communications - are performed by Unione Hotel Management Kft. (1123 Budapest Alkotás u. 55-61.)

For this purpose, personal data provided by the data subjects necessary for information purposes are transferred to Unione Hotel Management Kft.



The transferred data is used exclusively for the purpose of ensuring that those interested can receive timely, targeted information about promotions, offers, and news regarding hotels operated by the Unione Group.

Unione Hotel Management Kft. informs newsletter subscribers about current offers and special promotions of the hotels through newsletters as part of its marketing activities, always within the framework of the consent given by the data subjects, respecting their data protection rights.

We analyze the data and user habits of newsletter subscribers in order to communicate our offers to users in a personalized way through the contact details they have provided. The segmented data collection for marketing purposes qualifies as profiling according to Article 4, Point 4 of GDPR.

The data collection as described above qualifies as profiling, whereby the data voluntarily provided by the data subject, as well as the opening and clicking data measured on the website and in emails, may result in personalized marketing messages being sent to the data subjects.

Impact of profiling on the data subject: sending personalized marketing messages based on the activities of the data subjects.

Purpose of data processing:

Informing potential customers about current offers and promotions of hotels operated by the Unione Group

Legal basis for data processing:

Consent of the data subjects according to GDPR Article 6(1)(a)

Categories of data subjects:

Newsletter subscribers

Categories of personal data:

Name, email address, phone number

Duration of data processing for this purpose:

Until withdrawal by the data subject.

Is it mandatory to provide personal data, consequences of failure to provide data:

Not mandatory.

Without a name, we cannot address you.

Without an email address, we cannot notify you by email about promotions and current offers

Without an email address, we cannot send you a price quote

Without a phone number, we cannot call you back and coordinate personally

Recipients of personal data:

Email service provider, joint controller, data processor

Data processor:

Our company uses the assistance of an IT service provider for sending newsletters.



Data Processor's task: Storage of Newsletter Sending Database

ActiveCampaign, LLC
1 North Dearborn Street, 5th floor Chicago, IL 60602

By accepting this data processing notice, the data subject gives their explicit consent for the Data Processor to engage additional data processors as follows, in order to make the service more convenient and customized.

The Data Processor is headquartered in the United States, so the data transfer to them qualifies as a data transfer to a third country. However, the data processor has incorporated the standard contractual clauses proposed and approved by the European Commission into the data protection addendum of their general terms and conditions. In light of this, the data transfer to the data processor is considered to be provided with appropriate safeguards without requiring supervisory authority authorization, and therefore there is no legal obstacle to it.

Purpose of data processing: to provide electronic email sending functionality for newsletter delivery through the Postmark email servers of ActiveCampaign, LLC.

By accepting newsletter sending as a data processing purpose and consenting to the processing of their data, the data subject explicitly accepts that the Data Controller may engage additional data processors as follows, in order to make the service more convenient and customized:

Is there data transfer to a third country or international organization

We do not transfer data provided for this purpose to a third country (outside the EU) or international organization.

Information about automated decision-making:

No automated decision-making occurs in the processing of data for this purpose

VI/12 Data processing related to bookings (through email and web systems)

Our hotel provides the opportunity for online accommodation booking to make reserving a room at the Melea The Health Concept Hotel quick, convenient, and cost-free.

Purpose of data processing:

To make accommodation booking easier, cost-free, and more efficient.

Legal basis for data processing:

Consent of the data subjects according to GDPR Article 6(1)(a)

Categories of data subjects:

Natural persons booking accommodation

Categories of personal data:

Name, address, email address, phone number, bank card number, SZÉP card details, identification document data (document number, nationality, date of birth, name, address), vehicle license plate number.

Duration of data processing for this purpose:



2 years following the last day of the stay according to the booking.

Is it mandatory to provide personal data, consequences of failure to provide data:

No contract will be established regarding the hotel room.

Recipients of personal data:

Data processor

Data processor:

Our company uses the services of an IT provider for the online accommodation system as follows.

ActiveCampaign, LLC
1 North Dearborn Street, 5th floor Chicago, IL 60602

The Data Processor's headquarters is in the United States, so the data transfer to them qualifies as a transfer to a third country. However, Wildbit, LLC has incorporated the standard data protection clauses proposed and approved by the European Commission into the privacy supplement of its general terms and conditions. In light of this, the data transfer to Wildbit, LLC is considered to have adequate safeguards without requiring the authorization of a supervisory authority, so there is no legal obstacle to it.

Purpose of data processing: providing electronic mail sending functionality through ActiveCampaign, LLC's Postmark mail servers for sending informational messages necessary from the perspective of contract fulfillment. By accepting this privacy policy, the data subject expressly consents to the Data Controller and the Data Processor using additional data processors - in order to make the service more convenient and customized - as follows

Name of data processor	Registered office	Description of data processor task
Hostware Kft.	1149 Budapest, Róna utca 120-122	Customer management tasks when using the Hostware Front Office hotel system. The service provider's privacy policy is available at the following link: https://www.hostware.hu/sites/pdf/Adatkezelesi_tajekoztato.pdf
D-Edge Hospitality Solutions SAS	14-16 Boulevard Poissonnière, 75009 Paris, France	The purpose of the Revenue Management System connect service is to provide support for accommodation revenue optimization, that is, to enable automated, analysis-based management of prices and availability related to room bookings. This helps accommodations optimize their pricing policy.
Otp Bank Nyrt.	1051 Budapest, Nádor utca 16.	Data communication necessary for payment transactions between the merchant and the payment service provider's system, customer service assistance for users, confirmation of transactions, and fraud monitoring for the protection of users. The service provider's privacy policy is available at the following link: https://otpmobil.hu/adatkezelesi-tajekoztato/



Information about automated decision-making:

No automated decision-making occurs in the processing of data for this purpose

Other information related to data processing:

- By booking, the data subject also declares that their provided data is accurate and that they are at least 18 years old.
- We strive to help guests in preparing for their trip and reducing check-in time upon arrival with practical and relevant information, weather forecasts, program recommendations, and online check-in options, so we send them a pre-arrival email with information about the accommodation, travel, and program possibilities before their arrival. Based on the pre-arrival letter, the guest can fill out an online registration form to expedite their check-in at the accommodation upon arrival.
- Our company takes all necessary technical and organizational measures to avoid a possible data protection incident (e.g., damage or loss of files containing personal data, or unauthorized access to them). In the event of an incident, we maintain a record for the purpose of verifying the necessary measures and informing the data subject, which includes the scope of personal data affected, the circle and number of persons affected by the data protection incident, the time, circumstances, effects of the data protection incident and measures taken to remedy it, and other data specified by law prescribing data processing.
- Our company has concluded a data processing agreement for data processing tasks, in which the data processors undertake to mandatorily apply the data protection and data management guarantees prescribed by the data processing agreement in the event of engaging additional data processors. In light of this, we ensure the lawful processing of personal data in the case of the data processor as well.

VI/13. Data processing related to check-in

Purpose of data processing:

Enables the use of the given service. In addition, an important task is to ensure compliance with legal requirements for recording and storing appropriate data.

Legal basis for data processing:

Performance of contracts - GDPR Article 6(2) "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

Categories of data subjects:

Natural persons booking accommodation

Categories of personal data:

Name, address, email address, duration of stay, license plate number, payment method, passport number, ID card

Duration of data processing for this purpose:



Due to our reporting obligations, we must keep the data contained in the reports for 5 years following the calendar year of the check-in date;

Is it mandatory to provide personal data, consequences of failure to provide data:

Yes, without providing the data, we cannot provide the services.

Use of data processor:

We do not use a data processor.

VI/14. Use of supplementary services

We strive to fulfill our guests' requests to the best of our abilities. Accordingly, if we need the guest's personal data to fulfill the request, we record and process it accordingly.

Purpose of data processing:

Use and/or ordering of supplementary services based on our guests' requests. Such services may include (transfer service, laundry service, wake-up service, etc.)

Legal basis for data processing:

GDPR Article 6(1)(a), consent of data subjects

Categories of data subjects:

Natural persons booking accommodation

Categories of personal data:

Name, room number

Duration of data processing for this purpose:

Up to 3 days after the guest's departure

Is it mandatory to provide personal data, consequences of failure to provide data:

Not mandatory; in this case, we cannot provide the supplementary service.

Use of data processor:

If we need to involve a third party to provide the service (e.g., a taxi company for transfer service), we inform our guests when ordering the service. We always work with contracted partners who are obligated to comply with our data protection guidelines.



VI/15. Personal data processing related to satisfaction measurement

As a 5+ star hotel, our goal is to continuously provide high-quality services to our guests, which is why we request feedback from our guests about their experiences during their stay at our hotel.

Purpose of data processing:

Requesting feedback from hotel guests to further develop and improve our services.

Legal basis for data processing:

Legitimate interest of the hotel operator - GDPR Article 6(1)(f).

The legitimate interest specification: our hotel has a legitimate interest in receiving information to improve our services based on feedback.

Categories of data subjects:

Natural persons booking accommodation

Categories of personal data:

Name, gender, email address.

Duration of data processing for this purpose:

2 years following the last day of the stay according to the booking.

Is it mandatory to provide personal data, consequences of failure to provide data:

The data subject will not receive a satisfaction measurement questionnaire from our company.

Use of data processor:

Our hotel uses the assistance of an IT service provider for the online accommodation system as follows.

By accepting this data processing notice, the data subject gives their explicit consent for the Data Processor to engage additional data processors as follows, in order to make the service more convenient and customized.

VI/16. Data processing related to social media platform usage

The UNIONE SÁRVÁR KFT. uses the following social media platforms:

<https://www.facebook.com/MeleaTheHealthConcept/>

www.instagram.com/melea_health



The data you provide on our social media pages, such as comments, videos, images, likes, public messages, etc. are published by the social media platform, and we do not use or process them for any other purpose under any circumstances. We only reserve the right to delete content if it becomes necessary. We may share your content on our website if this is one of the features of the social media platform, and we may also communicate with you through the social media platform.

We would like to draw your attention to the fact that on our social media platforms, both our Company and the platform operator act as data controllers and perform data processing. In most cases, we cannot influence the activity of the operator, but where we can, we promote proper data processing according to the options available to us.

Purpose of data processing:

Supporting our communication and PR activities

Legal basis for data processing:

Legitimate interest of the hotel operator – GDPR Article 6(1)(f) for the purpose of facilitating communication.

Categories of data subjects:

Any natural person active on social media platforms

Categories of personal data:

links, images, videos, comments, profile name

Data processor:

Unione Hotel Management Kft.

For more information about the operator's data processing and how to object to data processing, please refer to the following privacy policies of the service providers:

- Facebook: <https://www.facebook.com/privacy/explanation>
- Instagram: <https://help.instagram.com/519522125107875>

The social media platform operator provides us with target group definitions that serve our advertising purposes. We only use anonymous target group definitions – for example, we define certain characteristics based on general demographic data, behavior, interests, and relationships. The social media platform operator uses these to deliver appropriate advertisements to members registered on the social network. The legal basis for this is the consent obtained from the members by the social media platform operator. If you wish to withdraw this consent, you can do so in the manner provided by the social media platform operator. In some cases, the social media platform operator may also use publicly available data for target group definition.

The legal basis for this is Article 6(1)(f) of the GDPR. We never use sensitive data categories listed in Articles 9 and 10 of the GDPR for defining target groups.

VI/17. Data processing related to the operation of internal whistleblowing systems



It is of paramount importance for the Company to ensure its lawful, ethical, and transparent operation and appropriate reputation, and to enforce the moral and ethical values and rules of conduct upheld by the Company with its employees and business partners.

Therefore, in accordance with the provisions of the Complaints Act, the Company operates an internal whistleblowing system aimed at ensuring compliance with legal requirements.

Purpose of data processing:

- Recording the report
- Investigating the report
- Remediating or terminating the conduct that is the subject of the report

Legal basis for data processing:

The data controller processes it lawfully under GDPR because it has a legal obligation to do so.

Legal obligation - Article 6(1)(c) of the GDPR: "processing is necessary for compliance with a legal obligation to which the controller is subject;"

Act XXV of 2023

Categories of data subjects:

Anyone entitled to make a report, including all employees of the Company, persons performing internship activities at the Company, and persons who are not employed by the Company but perform activities for the Company under a contract of mandate, contractor or other employment relationship, as well as those mentioned in the reports.

Categories of personal data:

name, email address, phone number, other personal data provided in the report

Duration of data processing for this purpose:

For 30 days following the report. If further measures are necessary based on the report, we keep the necessary data until the measure is taken; if official proceedings need to be initiated, we keep the data for an additional 1 year after the conclusion of the official or possible legal proceedings.

Is it mandatory to provide personal data, consequence of failure to provide data:

Yes

If the reporter cannot be identified, the feedback will not be investigated

Use of data processor:

We operate our whistleblowing system with an external service provider, which performs this task within a contractual framework. Name and address of external provider: Learnlab Kft. (6621 Derekegyház, Rákóczi u. 31.)

VI/18.RoomSome Loyalty Program data processing

Purpose of data processing: Melea The Health Concept hotel has joined the Roomsomeloyalty program (Roomsomeloyalty Program), which enables our guests to collect and redeem loyalty points, as well as receive personalized offers, discounts, and information. The purpose of data processing is to improve guest



experience, reward regular guests, and support marketing and communication activities within the framework of the program.

Legal basis for data processing:

- consent of the data subject (GDPR Article 6(1)(a)), and
- legitimate interest of Melea The Health Concept (GDPR Article 6(1)(f)) for maintaining and developing guest relationships.

Categories of personal data:

Name, email address, phone number, date of birth, country of residence, booking and stay information, as well as information related to loyalty points and membership level generated in the Roomsome system.

Duration of data processing:

Personal data is processed during the period of active participation in the loyalty program. If a user does not use their account for 24 months, their data will be automatically deleted, unless legislation prescribes a longer retention obligation.

Data processor:

The technical management and processing of data related to the loyalty program is carried out by ActiveCampaign, LLC (headquarters: 1 N Dearborn St 5th Floor, Chicago, IL 60602, USA) as a data processor, on behalf of the Data Controller.

ActiveCampaign is the operator of the marketing automation and communication system of the Roomsome Loyalty Program. Data transfer takes place based on data transfer mechanisms approved by the European Union (e.g., EU-USA Privacy Framework).

VII. Yours Rights

If you would like to exercise your rights mentioned above (request data transfer, deletion, correction, etc.), please contact us through any of our contact details or by filling out the form at the bottom of this chapter. You are entitled to the following rights:

VII/1. The right to information

VII/2. The right to access

VII/3. The right to rectification

VII/4. The right to erasure

VII/5. The right to restriction

VII/6. The right to data portability

VII/7. The right to object

VII/1. The right to information

We are obliged to provide appropriate sized, language, simple wording, and easily accessible information about the essential aspects of data processing (what, for what purpose, how, from when to when it is used,



etc.) - and the GDPR precisely defines the scope of necessary information. The information should preferably be provided before the collection of personal data. If this is not possible - for example, because the data is obtained from a third party - it should be done at the first possible opportunity.

You can read about the right to information in Articles 13-14 of the GDPR.

VII/2. The right to access

Ön tájékoztatást kérhet arról, hogy történik-e Önre vonatkozó adatkezelés, és ha igen, akkor mely adatait és milyen feltételekkel kezeljük. A lekérdezhető feltételek a fenti tájékoztatási jognál is részletezettek.

You can read about the right to access in Article 15 of the GDPR.

VII/3. The right to rectification

. You can notify us that the processed data is inaccurate and request what should be displayed instead. If you become aware that your data is inaccurate or incorrect, please notify us as soon as possible and we will correct it.

You can read about the right to rectification in Articles 16 and 19 of the GDPR.

VII/4. The right to erasure

You may request, in cases and under conditions specified by law, that we delete your data from the database. Such a case is, for example, if the personal data is no longer necessary for the purposes for which it was collected or otherwise processed, or if you withdraw your consent and there is no other legal basis for the processing.

Unfortunately, however, there are cases when we must refuse to delete data. One such case is if we are legally obliged to store the data (for example, data used for invoicing must be stored for a period of 8 years as a general rule in accordance with the relevant legislation), but we may also refuse based on legitimate interest - for example, for later proof - within the limitation period. And of course, beyond these examples, there are many cases where data processing despite objection is lawful. As with data protection in general, each case is unique and must be individually assessed to determine whether the refusal to delete data is lawful.

You can read about the right to erasure in Articles 17 and 19 of the GDPR.

VII/5. The right to restriction

You may request, in cases and under conditions specified by law, that we restrict the processing of your data for a specified period (even by law). Data subject to restriction may, except for exceptions specified by law, only be stored, no other operations may be performed on them. If the restriction is lifted, we will notify you.

You can request restriction in the following cases:

- You contest the accuracy of the personal data; in this case, the restriction applies for a period enabling the verification of the accuracy of the personal data.
- If the processing is unlawful, but you oppose the erasure of the data, you can request the restriction of their use instead.
- The controller no longer needs the personal data for the purposes of processing, but you require them for some legal proceedings.



- You have objected to the processing; in this case, the restriction applies for the period until it is verified whether the legitimate grounds of the controller override your legitimate grounds.

You can read about the right to restriction in Articles 18 and 19 of the GDPR.

VII/6. The right to data portability

You may request to receive the data processed about you in a structured, widely used, machine-readable format (e.g., .doc, .pdf, etc.), and you are entitled to transmit this data to another data controller without hindrance from the original controller. In other words, the GDPR regulatory framework makes it easier for data subjects to transfer their personal data from one controller to another. However, this is only possible if the processing is carried out by automated means.

You can read about the right to data portability in Article 20 of the GDPR.

VII/7. The right to object

You have the right to object to the processing of your data in certain cases. In case of objection, we cannot process your personal data unless there are compelling legitimate reasons that override your interests, rights, and freedoms, or that are necessary for potential legal claims, official or court proceedings.

In certain cases, you have the right to request the exclusion of automated decision-making if you wish this not to apply to you. The primary condition for this is that it is not necessary for the conclusion or performance of a contract between you and us, and that the law does not require automated decision-making in the given case.

You can read about the right to object and automated decision-making in Articles 21-22 of the GDPR.

VIII. Where to seek legal remedies

First, please contact us with confidence; we will definitely work to solve your problem! If this is not successful, or you do not wish to do so, you can contact the data protection authority or file a lawsuit in court.

Contact details of the Hungarian data protection supervisory authority:

National Authority for Data Protection and Freedom of Information

Postal address:	1363 Budapest, Pf.: 9.
Address:	1055 Budapest, Falk Miksa u. 9-11.
Phone:	+36 (1) 391-1400
Fax:	+36 (1) 391-1410
E-mail:	ugyfelszolgalat@naih.hu
Website:	https://naih.hu

The right to take legal action

In case of violation of your rights as a data subject, you may also take legal action against the data controller. The lawsuit can be initiated at the court having jurisdiction based on your place of residence or stay, at your choice.

IX. Validity of this policy

This policy is valid from October 1, 2025, until revoked