

BOTANIQ Budai Klub

Public Privacy Notice

1. Purpose of this Notice

The purpose of this Notice is to provide members, membership applicants, guests, legal representatives, enquirers and other data subjects with information on the processing of personal data by BOTANIQ Budai Klub, operated by Tusculanum Hegyvidék Üzemeltető Kft.

Details of the Controller:

Name of the Controller: Tusculanum Hegyvidék Üzemeltető Kft.

Address of the Controller: 1026 Budapest, Pasaréti út 122.-124.

Telephone number of the Controller: +36 30 731 7968

Email address of the Controller: info@botaniqubudaiklub.hu

This Notice shall take effect on 03 October 2026 and shall remain in force until further notice or until revoked.

2. Principles of personal data processing

We have designed the personal data processing operations of Tusculanum Hegyvidék Üzemeltető Kft. to ensure that they always comply with the principles laid down in the applicable legislation. These principles must also be taken into account when this Notice is amended in the future. In particular, we guarantee compliance with the following principles in the course of processing personal data.

2.1. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2.2. Necessity and proportionality

A fundamental right may only be restricted where such restriction is necessary and proportionate. Necessity means that the processing of personal data is strictly necessary to achieve the purpose of the processing. Proportionality sets the limits of this necessity by requiring that any restriction of fundamental rights and freedoms necessary for the processing must also be proportionate to the objective pursued.

The Fundamental Law of Hungary provides that a fundamental right may be restricted in order to ensure the exercise of another fundamental right or to protect a constitutional value, to the extent strictly necessary, in proportion to the objective pursued and with respect for the essential content of that fundamental right.

2.3. Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes and must not be further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1) of the GDPR, shall not be considered incompatible with the initial purposes.

2.4. Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

2.5. Accuracy

Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

2.6. Storage limitation

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods only insofar as they will be processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, subject to implementation of the appropriate technical and organisational measures required by that Regulation in order to safeguard the rights and freedoms of the data subjects.

2.7. Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, through the use of appropriate technical or organisational measures.

2.8. Accountability

The controller is responsible for compliance with the data protection rules and must be able to demonstrate such compliance.

3. Legal bases for processing personal data

We process personal data on the following legal bases, taking into account the specific rules highlighted below.

3.1. Consent of the data subject

The data subject has given consent to the processing of their personal data for one or more specific purposes. Consent must be freely given and must, in every case, be given by an affirmative action on the part of the person giving consent.

3.2. Performance of a contract

Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

3.3. Legal obligation

Processing is necessary for compliance with a legal obligation to which the controller is subject. We process data on the legal basis of a legal obligation only where processing is required by law. We do not rely on a legal obligation as the legal basis for processing where legislation provides for processing in permissive rather than mandatory terms.

3.4. Vital interests

Processing is necessary in order to protect the vital interests of the data subject or of another natural person. An important consideration when selecting this legal basis is that processing on the basis of vital interests is temporary and may continue only for as long as the vital interest exists. We separately regulate the arrangements for processing the data once the vital interest has ceased to exist.

3.5. Public interest or official authority

In this case, processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Our company is not a public authority and does not process data in the public interest; therefore, we do not process data on this legal basis.

3.6. Legitimate interests

Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the

data subject which require protection of personal data, in particular where the data subject is a child. We frequently process personal data on this legal basis.

Where personal data are processed on the basis of legitimate interests, a balancing test must be carried out in every case to assess the proportionality and necessity of the impact on, and restriction of, the data subject's fundamental rights and freedoms.

4. Rights of data subjects

We have designed our personal data processing operations to ensure that the rights of data subjects are not infringed and that data subjects can always exercise those rights within the limits laid down by the GDPR and the applicable legislation. Data subjects have the following rights:

4.1. Right to be informed

The controller must provide information on the essential aspects of the processing (what data are used, for what purpose, how and for how long, etc.) in an appropriate size and language, using plain language and in an easily accessible form. The GDPR precisely specifies the information to be provided. Wherever possible, the information must be provided before personal data are collected. If this is not possible, for example because the data are obtained from a third party, the information will be provided at the earliest possible opportunity.

The right to be informed is governed by Articles 13–14 of the GDPR. The provision of information to data subjects is addressed in a separate section.

4.2. Right of access

The data subject may request information as to whether personal data concerning them are being processed and, if so, which of their data we process and under what conditions.

The controller must provide the data subject with a copy of the personal data undergoing processing, free of charge on the first occasion. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs; the fee applicable from time to time must be specified in the privacy notice. Where the data subject submits the request by electronic means, the information must be provided in a commonly used electronic form, unless otherwise requested by the data subject. The right to request a copy must not adversely affect the rights and freedoms of others.

4.3. Right to rectification

The data subject may notify the controller that the data being processed are inaccurate and request that specified information be recorded instead. The controller may refuse to rectify the data only in cases specified by law. The data subject has the right to obtain from the controller, upon request and without undue delay, the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

4.4. Right to erasure ("right to be forgotten")

The data subject may request that their data be erased from the database in the cases and subject to the conditions laid down by law. This may be the case, for example, where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, or where the data subject withdraws consent and there is no other legal basis for the processing.

There are cases in which erasure of the data must be refused. One such case is where the controller is required by law to retain the data (for example, data used for invoicing must, as a general rule, be retained for 8 years in accordance with the applicable legislation). Erasure within the limitation period may also be

refused on the basis of legitimate interests, for example to enable evidence to be produced at a later stage. Beyond these examples, there are numerous other cases in which processing despite an objection is lawful. As is generally the case in data protection, each matter is individual and requires a case-by-case assessment of whether refusing to erase the data is lawful.

Upon the data subject's request, the data must be erased without undue delay where any of the grounds specified by law applies.

Where the controller has made personal data public in the course of processing and is obliged to erase them at the data subject's request, the controller must, taking account of available technology and the cost of implementation, take reasonable steps, including technical measures, to ensure that the data are also permanently erased by other controllers. The controller must inform the controllers processing the data that the data subject has requested the erasure by those controllers of any links to, or copies or replications of, the personal data in question.

The above obligation to erase does not apply and need not be fulfilled where processing is necessary under the conditions specified by law.

4.5. Right to restriction of processing

The data subject may request that we restrict the processing of their data for a specified period, which may also be prescribed by law, in the cases and subject to the conditions laid down by law. Data subject to restriction may only be stored, and no other operations may be performed on them, except in the cases specified by law. The data subject must be notified when the restriction is lifted.

The controller shall inform the data subject whose request led to the restriction of processing before that restriction is lifted.

4.6. Right to data portability

The data subject may request to receive the data concerning them that are being processed in a structured, commonly used and machine-readable format (e.g. .doc, .pdf, etc.), and has the right to transmit those data to another controller without hindrance from the original controller. In other words, the GDPR framework makes it easier for the data subject to transfer their personal data from one controller to another. However, this is possible only where the processing is carried out by automated means and is based on consent pursuant to Article 6(1)(a) or Article 9(2)(a) of the GDPR, or on a contract pursuant to Article 6(1)(b) of the GDPR.

Where the data subject so requests and it is technically feasible, the data must be transmitted directly between the controllers.

The right to data portability does not apply where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The right to data portability must not adversely affect the rights and freedoms of others.

4.7. Right to object

The data subject has the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them which is based on Article 6(1)(e) or (f), including profiling based on those provisions. In this case, the personal data must no longer be processed unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or grounds relating to the establishment, exercise or defence of legal claims.

In this case, a balancing test must be carried out, and processing may take place only if the legitimate grounds justify the overriding priority referred to above.

Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing of personal data concerning them for such purposes, including profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing of personal data for direct marketing purposes, the personal data must no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, the above right must be explicitly brought to their attention and must be presented clearly and separately from any other information.

In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise the right to object by automated means using technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject has the right, on grounds relating to their particular situation, to object to processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Where an objection is justified, further processing of the data is prohibited.

4.8. Automated individual decision-making, including profiling

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

Such decisions must not be based on the special categories of personal data referred to in Article 9(1), unless Article 9(2)(a) or (g) applies and suitable measures have been taken to safeguard the data subject's rights, freedoms and legitimate interests.

5. Personal data processing by BOTANIQ Budai Klub

The table below summarises the individual personal data processing activities associated with the operation of BOTANIQ Budai Klub. For each purpose of processing, the table sets out the categories of personal data processed to achieve that purpose, the legal basis for processing under the GDPR and the period for which the Controller processes the personal data. The Controller processes personal data solely for the purposes specified in the table, to the extent and for the period necessary to achieve the relevant purpose.

Purpose of processing	Categories of data processed	Legal basis – reference and description	Duration of processing
Handling enquiries and requests for information and quotations	Name, email address, telephone number, content of the enquiry and any other data provided by the data subject to enable a response.	Article 6(1)(b) of the GDPR – processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.	Until the enquiry is closed; if a contractual relationship is established, the data may continue to be processed as part of the related processing activity.
Assessment of membership applications and establishment and maintenance of the membership relationship	Surname, first name, place and date of birth, permanent residential address, country, postcode, city, road / street, house number / building / door, telephone number, email	Article 6(1)(b) of the GDPR – processing is necessary in order to take steps at the request of the data subject prior to entering into a contract and to perform the membership agreement.	For rejected applications, until the assessment is concluded and for as long as necessary to pursue any claims; where membership is established, for the

Purpose of processing	Categories of data processed	Legal basis – reference and description	Duration of processing
	address, alternative billing address, application and contractual declarations, place, date, signature, membership category, commencement date and duration of membership, membership and payment status.		duration of the membership relationship and thereafter until expiry of the limitation period for civil claims arising from it.
Administration of a minor applicant's membership and documentation of legal representation / consent	The minor's membership data; the legal representative's name, relationship to the applicant, telephone number, email address, residential address, declaration, date and signature.	Article 6(1)(b) of the GDPR – processing is necessary to enter into and perform the minor's membership agreement.	For the same period as the documentation relating to the application / membership relationship.
Verification of membership entitlement, administration of membership cards or digital membership identifiers and admission	Name, membership identifier or card data, membership status, the fact that an identity document has been presented and data relating to lost identifiers or identifiers used without authorisation.	Article 6(1)(b) of the GDPR – processing necessary for the performance of the membership agreement. When investigating misuse, Article 6(1)(f) of the GDPR – the controller's legitimate interest in the secure operation of the membership and admission system and in the prevention and investigation of misuse.	For the duration of the membership relationship; in cases of misuse, following closure of the matter, until expiry of the limitation period for legal claims arising from it.
Processing of a Member's photograph for identification and admission purposes	Image / photograph and the membership identifier linked to the photograph.	Article 6(1)(b) of the GDPR – the photograph in the membership and admission system is necessary for the performance of the membership agreement.	Until termination of the membership relationship or, if earlier, until the identification purpose ceases to apply.
Contact and notifications relating to the membership relationship	Name, email address, telephone number, postal address, content of communications and notifications, delivery data.	Article 6(1)(b) of the GDPR – processing necessary for the performance of the membership agreement.	For the duration of the membership relationship; for communications having legal effect, until expiry of the limitation period for claims arising from them.
Advance notification, registration and admission of Guests and	Data necessary to identify the Guest, data of the inviting Member, date of the visit, admission entitlement and Guest	Article 6(1)(f) of the GDPR – the controller's legitimate interest in ensuring a membership-based admission system,	Until the visit and the related financial settlement are concluded; in cases of misuse or a legal

Purpose of processing	Categories of data processed	Legal basis – reference and description	Duration of processing
administration of Guest Day Passes	Day Pass data. The precise guest data fields cannot be determined from the available documents.	managing capacity and ensuring the safe operation of the Club. For contractual processing relating to a fee-paying Guest Day Pass, Article 6(1)(b) of the GDPR – performance of the contract.	dispute, until expiry of the limitation period for claims arising from them.
Booking and provision of tennis and padel courts, PDR and other services subject to advance booking or a separate fee	Name, membership identifier, contact details, subject, date, time and duration of the booking, necessary participant / guest data, service fee and payment data.	Article 6(1)(b) of the GDPR – processing is necessary to enter into and perform the contract relating to the booking / order.	Until the service has been provided and the financial settlement concluded; for contractual claims, until expiry of the limitation period for the claim; for accounting documents, until the end of the statutory accounting retention period.
Authorisation and arrangement of the use of PDR and other Club spaces for events	Name, contact details and membership data of the organising Member; nature, date, time and duration of the event, number of participants; contact details of external contributors, their activities, equipment to be installed and, where necessary, data required to evidence permits, professional authorisations and liability insurance.	Article 6(1)(b) of the GDPR – preparation and performance of the contract with the organiser. For contact persons of external contributors, Article 6(1)(f) of the GDPR – the controller's legitimate interest in ensuring that the event is conducted safely and in accordance with the applicable rules.	Until the event and the financial settlement are concluded; in contractual matters or legal disputes, until expiry of the limitation period for claims arising from them.
Advance registration and authorisation of external personal trainers or sports instructors	Name, contact details, data of the inviting Member and, where necessary, data required to evidence professional qualifications / authorisations and liability insurance, authorisation status.	Article 6(1)(f) of the GDPR – the controller's legitimate interest in verifying the safety, lawfulness and appropriate professional conditions of external professional services provided on the Club's premises.	For the period necessary for authorisation and the related use of the Club; in the event of damage or a legal dispute, until expiry of the limitation period for claims arising from it.
Investigation of breaches of the Club Rules and misuse; suspension of membership or admission	Name and identification data, membership / guest status, contact details, time, place and circumstances of the event, statements, related documents, measures,	Article 6(1)(f) of the GDPR – the controller's legitimate interest in ensuring the safe operation and proper use of the Club, protecting the rights of other persons	Until the matter is closed and thereafter until expiry of the limitation period for legal claims arising from it.

Purpose of processing	Categories of data processed	Legal basis – reference and description	Duration of processing
entitlement and exclusion	decisions and, where necessary, data relating to damage.	and of the Club, investigating misuse and establishing, exercising or defending legal claims.	
Handling extraordinary events, accidents and emergencies	Data necessary to identify and contact the data subject, time, place and circumstances of the event; where necessary, health data relating to the event.	Depending on the circumstances of the case, Article 6(1)(d) of the GDPR – processing is necessary to protect the vital interests of the data subject or of another natural person; or Article 6(1)(f) of the GDPR – the controller's legitimate interest in documenting the security event and handling legal claims. Where special categories of personal data are involved, an appropriate condition under Article 9 of the GDPR must also be met.	Until the event is closed and thereafter until expiry of the limitation period for any legal claims.
Invoicing and accounting for membership fees, Guest Day Passes and services subject to separate fees	Name, billing address, description of the service, consideration, invoice / accounting document data and data necessary for payment.	Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the controller is subject, in particular accounting and tax obligations.	Retention period under Section 169 of Act C of 2000 on Accounting: at least 8 years.
Handling complaints	Name, contact details, membership / guest data, content of the complaint, dates of submission and response, related documents and measures.	Article 6(1)(c) of the GDPR – compliance with a statutory obligation to handle complaints; for other enquiries, Article 6(1)(f) of the GDPR – the controller's legitimate interest in investigating the complaint and handling legal claims.	For complaints and responses required to be retained by law, the period prescribed by the applicable rules on complaint handling; in the event of a legal dispute, until expiry of the limitation period for the claims.
Handling and return of lost property	Name, contact details, description of the item found, circumstances in which it was found and handed over, and data necessary to verify entitlement to claim the item.	Article 6(1)(c) of the GDPR – where processing is necessary for compliance with a legal obligation; for other processing of contact details, Article 6(1)(f) of the GDPR – the legitimate interests of the controller and the entitled person in returning the item found to the person entitled to it.	Until the item is handed over or the procedure concerning the item found is concluded; in the event of a legal dispute, until expiry of the limitation period for the claims.

Purpose of processing	Categories of data processed	Legal basis – reference and description	Duration of processing
Video surveillance	Images of individuals, movements and events visible in the recording.	Article 6(1)(f) of the GDPR – the controller's legitimate interest in protecting persons and property, ensuring the safe operation of the Club and preventing, detecting and investigating unlawful acts and incidents involving damage.	A maximum of 30 days under the video surveillance policy.

6. Processing of recordings from cameras operating on the premises of BOTANIQ Budai Klub

A camera system has been installed and put into operation on the premises of BOTANIQ Budai Klub to protect life, physical integrity and property (hereinafter referred to as the cameras). The cameras record images. The reasons for their installation are that several items of high-value equipment and machinery are located on the Club's premises and that protecting guests' physical integrity and valuables is a priority. The rules applicable to the camera system and the balancing test are set out in a separate notice.

7. Processors and other recipients

To operate BOTANIQ Budai Klub, provide services associated with the membership relationship and comply with its statutory obligations, the Controller engages external service providers to whom personal data necessary for the performance of the relevant task or service may be disclosed.

Where an external service provider processes personal data on behalf of the Controller and in accordance with its documented instructions, it acts as a **processor** within the meaning of Article 28 of the GDPR. The Controller engages only processors that provide sufficient guarantees that processing will comply with the requirements of the GDPR and ensure appropriate protection of the rights of data subjects.

Some service providers independently determine the purposes and means of processing the personal data disclosed to them and also process personal data in order to comply with their own statutory obligations. These service providers act as **independent controllers**. In such cases, the relevant service provider is responsible for further processing of the personal data in accordance with its own privacy notice.

The Controller discloses to processors and other recipients only the personal data necessary for the performance of the relevant task or service or for compliance with a statutory obligation.

Purpose of processing	Name and address of the processor / recipient	Role under the GDPR	Processing activity / processor task
Operation of IT systems and performance of system administration tasks	SMBinfo Kft. 1076 Budapest, Péterfy Sándor utca 7, mezzanine, door 1	Processor	IT services, system operation and technical support relating to the Club's membership and software application system.

Purpose of processing	Name and address of the processor / recipient	Role under the GDPR	Processing activity / processor task
Compliance with accounting and bookkeeping obligations	Corient Accounting Kft. 1026 Budapest, Pasaréti út 122-124	Processor	Processing of accounting documents and performance of bookkeeping and related accounting tasks.
Execution of payment card transactions	Hungarian Branch of Worldline Financial Services (Europe) Ltd., 1034 Budapest, Tímár utca 20, 1st floor	Independent controller / payment service provider	Authorisation, processing and settlement of payment card transactions and compliance with statutory obligations applicable to the payment service provider.
Execution of bank transfers and other payment transactions	GRÁNIT Bank Nyrt., 1134 Budapest, Váci út 17.	Independent controller / payment service provider	Maintenance of bank accounts, execution of transfers and other payment transactions, and compliance with statutory obligations applicable to the bank.
Earning and redeeming points under the BOTANIQ Benefit Loyalty Program	BDPST Hotel Management Zrt., 1026 Budapest, Pasaréti út 122–124.	Independent controller	Operation of the BOTANIQ Benefit Loyalty Program, identification of the member participating in the program and processing of data relating to transactions at the Club that qualify for earning or redeeming points.
Technical delivery of newsletters and management of the subscriber database	The Rocket Science Group LLC d/b/a Mailchimp 675 Ponce De Leon Avenue NE, Suite 5000, Atlanta, GA 30308, USA	Processor	Technical management of the subscriber database, sending newsletters, handling unsubscribe requests and processing related technical data.

7.1. Transfers of personal data to third countries

The Controller endeavours to ensure that personal data are processed within the European Economic Area (EEA). However, the operations of certain IT, communications or social media service providers engaged by the Controller may involve the transfer of personal data outside the EEA to so-called third countries, or access to personal data from third countries.

The Controller uses the Mailchimp service provided by The Rocket Science Group LLC d/b/a Mailchimp (675 Ponce De Leon Avenue NE, Suite 5000, Atlanta, GA 30308, USA) to send newsletters. Mailchimp is a processor established in the United States of America, and its servers are located in the United States; therefore, the use of the service involves the transfer and processing of personal data outside the European Economic Area. Transfers of personal data to the United States of America take place in accordance with

the requirements of Chapter V of the GDPR. Mailchimp's service provider is certified under Intuit's EU–US Data Privacy Framework program; therefore, the transfer is based on the relevant adequacy decision of the European Commission. Mailchimp's data processing terms also include the Standard Contractual Clauses (SCC) adopted by the European Commission, which apply where the transfer cannot take place on the basis of the Data Privacy Framework. Mailchimp processes personal data on behalf of the Controller and in accordance with its instructions, to the extent necessary to provide the service.

7.2. Transfers of personal data to legal representatives, authorities and other bodies

The Controller may also disclose personal data to its legal representative, lawyer, expert or insurer, to a court, authority or investigating authority, or to another body authorised to act under the law, where the disclosure is necessary for the establishment, exercise or defence of a legal claim, the resolution of a legal dispute or compliance with a legal obligation to which the Controller is subject. Where disclosure is based on a legal obligation, the legal basis for processing is Article 6(1)(c) of the GDPR. Where disclosure relates to the exercise or defence of legal claims, the legal basis may, depending on the circumstances of the case, be legitimate interests under Article 6(1)(f) of the GDPR. In such cases, too, the Controller discloses only the personal data necessary for the relevant proceedings, request or legal claim.

8. Data security measures

When processing personal data, the Controller pays particular attention to data security and, in accordance with the requirements of Article 32 of the GDPR, implements technical and organisational measures that ensure an appropriate level of protection, taking into account the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of natural persons.

When designing data security measures, the Controller takes into account, in particular, the categories and volume of personal data processed, the manner of processing, the IT systems used, the persons who have access to the data and the potential risks arising from unauthorised access, alteration, disclosure, loss or destruction.

The Controller takes appropriate measures to maintain the confidentiality, integrity and availability of personal data. Only employees, other persons involved in the processing and processors who need to know the relevant data to perform their duties may have access to personal data. The Controller determines access rights according to the tasks to be performed and endeavours to ensure that each authorised person has access only to the data necessary for their work.

To protect personal data processed in electronic form, the Controller implements, in particular and according to the characteristics of the relevant system, appropriate user identification and access rights management solutions, password protection, access controls, data backup and recovery solutions, and measures to prevent unauthorised use of IT systems and devices. The Controller also ensures that access to personal data is appropriately modified or revoked when a job role, task or legal relationship changes or ends.

The Controller stores and handles paper documents containing personal data in a manner that prevents unauthorised persons from gaining access to them. The Controller ensures that documents containing personal data are appropriately stored, transmitted and archived, and securely destroyed after the retention period has expired.

When selecting processors and other service providers that have access to personal data, the Controller also takes data security requirements into account and sets out appropriate data protection and data security

obligations in its contracts with processors. The processor may process personal data made available to it only in accordance with the Controller's documented instructions and must ensure that the data are appropriately protected.

The Controller reviews the adequacy of the technical and organisational measures implemented as necessary, particularly where there are material changes to processing operations, the technology used, the service providers engaged or the risks associated with the processing. The Controller's objective is for data security to be a requirement continuously observed throughout the entire period of personal data processing, rather than a one-off measure.

9. Handling personal data breaches

Under Article 4(12) of the GDPR, a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A personal data breach may therefore include, in particular, the loss of a document, device or storage medium containing personal data, the sending of personal data to an incorrect recipient, unauthorised access to an IT system, unauthorised transfer or disclosure of personal data, or a breach affecting the availability of personal data that may pose a risk to data subjects.

The Controller applies an internal procedure for detecting, handling and documenting personal data breaches. The Controller's staff and persons involved in the processing must immediately report any personal data breach they detect or suspect to the person designated for this purpose by the Controller or to its data protection contact person, so that investigation of the incident and implementation of the necessary measures can begin without undue delay.

The Controller investigates every personal data breach of which it becomes aware. In doing so, it establishes, in particular, the nature and cause of the breach, the categories of personal data and data subjects affected, the likely consequences of the breach and the risk that the event may pose to the rights and freedoms of the natural persons concerned. Depending on the nature of the breach, the Controller immediately takes the necessary technical, organisational and other measures to end the breach, mitigate any adverse consequences, prevent further unauthorised access to personal data and prevent the recurrence of similar events.

In accordance with Article 33(5) of the GDPR, the Controller documents all personal data breaches, including the facts relating to the breach, its effects and the remedial action taken. The documentation is maintained in a manner that enables the supervisory authority to verify compliance with the GDPR requirements relating to the handling of personal data breaches.

Where, based on the Controller's assessment, a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the Controller shall, in accordance with Article 33 of the GDPR, notify the National Authority for Data Protection and Freedom of Information of the breach without undue delay and, where feasible, no later than 72 hours after becoming aware of it. Where notification is not made within 72 hours, the Controller shall also provide the supervisory authority with the reasons for the delay.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons concerned, the Controller shall also inform the data subjects without undue delay, subject to the conditions laid down in Article 34 of the GDPR. The communication shall describe in clear and plain language at least the nature of the personal data breach, the contact details of the data protection contact person, the likely consequences of the breach and the measures taken or proposed by the Controller to address the breach and mitigate its consequences.

No separate communication will be made to data subjects where any of the exceptions specified in Article 34 of the GDPR applies, in particular where the Controller has implemented appropriate technical and

organisational protection measures that rendered the personal data affected by the breach unintelligible to unauthorised persons, or where the Controller has taken measures following the breach as a result of which the high risk is no longer likely to materialise.

Where a personal data breach occurs at a processor, the processor must notify the Controller of the breach without undue delay and provide the information and cooperation necessary to investigate the breach, assess the risks, document the incident and make any necessary notification to the supervisory authority and communication to data subjects.

10. Rules on the processing of personal data relating to cookies

A cookie is a small text file placed on your computer when you visit a website. Cookies perform a variety of functions, including collecting information, remembering user preferences and enabling the website owner to understand user habits in order to improve the user experience. You may manage your cookie preferences at any time through your browser settings. Further information on cookies is provided when you access our website.

11. Provision of information to data subjects

Under the European Union's General Data Protection Regulation (GDPR), which is legislation in force and with which compliance is mandatory, we are obliged to provide you with information on the processing of your data. The privacy notice will specify the types of data we collect, the purposes for which the data are processed, the periods for which the data are stored, the legal basis for access to the data, the legitimate interests relating to the data and your rights regarding the processing of your data. Through this Notice, we ensure that the processing is fully consistent with the requirements of the GDPR in all respects and that you can become familiar with the principles governing the secure and responsible processing of your data.

It is important to distinguish, and to make separate provision when preparing information relating to individual processing activities for, cases in which data are processed on the basis of the Data Subject's consent or on another legal basis, as well as cases in which data are collected directly from the data subject or obtained from another source.

The GDPR itself imposes different information obligations on controllers: where the data subject provides their data directly, appropriate information must already be provided when processing begins.

There are, however, exemptions from the obligation to provide information. These include cases where fulfilling that obligation "proves impossible" or "would involve disproportionate effort". This does not mean, however, that we may rely on an exemption merely by making a general statement referring to those grounds. Whenever we consider that such grounds may exist, we must examine, in light of the characteristics of the particular processing activity, whether reliance on those grounds would restrict the rights, freedoms and legitimate interests of data subjects beyond what is necessary and proportionate.

12. Available remedies

Where a data subject considers that the Controller has infringed the statutory provisions on the protection of personal data in the course of processing their personal data, the data subject has the right to lodge a complaint with the supervisory authority or to request the initiation of a data protection authority procedure before the National Authority for Data Protection and Freedom of Information (NAIH).

National Authority for Data Protection and Freedom of Information

Registered office: 1055 Budapest, Falk Miksa utca 9–11.

Postal address: 1363 Budapest, P.O. Box 9.

Telephone: +36 (1) 391-1400

Email: ugyfelszolgalat@naih.hu

The data subject also has the right to seek a judicial remedy where they consider that their rights under the GDPR have been infringed in the course of processing their personal data. The data subject may bring proceedings against the Controller and seek judicial enforcement of their rights in accordance with the GDPR and the applicable Hungarian legislation.

Dated: Budapest, 3 October 2026.

Tusculanum Hegyvidék Üzemeltető Kft.