

PRIVACY POLICY

1. Data Controller

Name: Kultúrpark Zrt.

Address: 1095 Budapest, Fábián Juli tér 1.

Representative of the Data Controller: András Pálffy

Data protection contact of the Data Controller: adatvedelem@budapestpark.hu

This Privacy Policy constitutes a unilateral undertaking by the Data Controller pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and the applicable national legislation.

The Data Controller may unilaterally amend and/or withdraw this Privacy Policy at any time, subject to the simultaneous information of the data subjects. Such information is provided by publication on the website or — depending on the nature of the change — by direct notification of the data subjects.

2. Purposes of data processing

2.1 Records of IT system access management

Identification of users and control of access.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in supervising and protecting its data assets and in controlling access to them.

Scope of the data processed: System name, access level, user ID, user activity log file, email address

Planned deadline for data processing: Until the last working day of January of the 3rd calendar year following the termination of the employment contract, or until the data subject objects.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.2 Operation of an electronic video surveillance system

Operation of a camera system at the Data Controller's work sites.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in protecting its assets and controlling access.

Scope of the data processed: Facial and body image

Planned deadline for data processing: A maximum of 15 days.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: Security guard

2.3 Management and filing of contracts

Filing of the contracts related to the Data Controller's activities; recording and keeping up to date the data of the contracting party's contact persons upon the conclusion of the contract, as well as the data of the contracting party's authorised representatives.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in keeping records of the data of contact persons.

Scope of the data processed: Name, phone number, position, email address, signature

Planned deadline for data processing: Until the last working day of January of the 4th year following the termination of the contract, or until the data subject objects.

Source of data collection: Data provided by the data subject, the data subject's employer, or the data subject's partner

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.4 Handling requests for quotations

Recording and answering questions and requests for quotations received at the Organisation's central email address or at a colleague's personal email address; issuing quotations.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in pre-contractual contact and in keeping records of the data of contact persons.

Scope of the data processed: Name, address, email address, phone number, unique identifier

Planned deadline for data processing: Until the last working day of January of the 1st year following the receipt of the request for a quotation, or until the data subject objects.

Source of data collection: Data provided by the data subject, the data subject's employer, or the data subject's partner

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.5 Management and registration of orders

The Data Controller keeps records of incoming and outgoing orders.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in pre-contractual contact and in keeping records of the data of contact persons.

Scope of the data processed: Name, address, email address, phone number, unique identifier

Planned deadline for data processing: Until the last working day of January of the 5th calendar year following the date of the order.

Source of data collection: Data provided by the data subject, the data subject's employer, or the data subject's partner

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.6 Identification and registration of persons entering the premises

Processing of data related to the entry to the premises of persons who do not hold an organisational access card; admission of guests and external vehicles.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in supervising the premises, protecting its assets, preventing accidents, and enabling comprehensive action in the event of an emergency.

Scope of the data processed: Name, number of the identification document, company name

Planned deadline for data processing: 6 months

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: Security guard

2.7 Registration for events

Management of registrations related to corporate events and family day events organised by the Data Controller.

Legal basis for data processing: Consent of the data subject (Article 6(1)(a) GDPR).

Scope of the data processed: Name, company name, position, email address, phone number, number of adult guests, number of child guests (under 16)

Planned deadline for data processing: Until the withdrawal of the data subject's consent.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: Event organiser, photo and video service provider, hostess service provider, property protection service provider

2.8 Photo and video documentation of events

The Data Controller takes photo and video recordings of the events it organises, which it may publish on its website and Facebook page and store in its own databases.

Legal basis for data processing: Consent of the data subject (Article 6(1)(a) GDPR).

Scope of the data processed: Facial and body image

Planned deadline for data processing: Until the withdrawal of the data subject's consent.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.9 Management of declarations of liability

In connection with activities subject to a licence or professional qualification, the Data Controller has the subcontractors performing such activities complete declarations of liability, which it keeps on record.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in keeping records of the declarations of liability related to licensed activities performed on its premises.

Scope of the data processed: Name, number of the identification document, licence or certificate number, signature

Planned deadline for data processing: Until the last working day of January of the 5th year following the termination of the legal relationship with the subcontractor.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.10 Photo and video documentation of events, and media communication for promotional purposes

The Data Controller produces photo and video recordings, promotional videos and live Facebook broadcasts of its public events, which it may publish on its website and social media pages, use in advertising, and store in its own databases.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in the effective and personalised promotion of the organisation.

Scope of the data processed: Facial and body image

Planned deadline for data processing: Until the data subject objects.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: IT service provider, web service provider, G Suite, social media platforms

2.11 Issuing invoices and the mandatory documentation related to the performance of the service, and storing the data for compliance with the Accounting Act

Issuing invoices related to the Data Controller's catering and event organisation activities, and issuing the mandatory documentation related to the performance of the service.

Legal basis for data processing: Compliance with a legal obligation to which the Data Controller is subject (Article 6(1)(c) GDPR).

Scope of the data processed: Billing name and address, email address, phone number, tax number

Planned deadline for data processing: 8 years

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: Authority, contracted accountant, invoicing service provider

2.12 Live or recorded television broadcasts

Budapest Park provides the press and the media, acting as independent data controllers, with the opportunity to make on-site recordings and broadcasts.

Legal basis for data processing: The independent data controller status of the press and the media.

Scope of the data processed: Budapest Park does not process any data.

Planned deadline for data processing: Budapest Park does not process any data.

Source of data collection: -

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.13 Provision of the venue to external partners for making video and photo recordings

Budapest Park provides its partners, performers, event sponsors and venue hirers with the opportunity to make photo and video recordings or live broadcasts at public events.

Legal basis for data processing: As set out in the partner's privacy notice.

Scope of the data processed: Budapest Park does not process any data.

Planned deadline for data processing: Budapest Park does not process any data.

Source of data collection: -

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.14 IT data backup

Operation of IT systems and infrastructure, including the operation of workstations, servers and network elements, the archiving and backing up of data, and their restoration in the event of a disaster.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in regularly backing up and archiving the data of its IT systems in order to maintain business continuity.

Scope of the data processed: All categories of digital data collected or processed by the Organisation

Planned deadline for data processing: Backups of the IT system are stored for 10 days; archived data are stored for 5 years.

Source of data collection: Data from the Data Controller's IT systems

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: System operator

2.15 Operation of an electronic video surveillance system

Protection of the security of the Data Controller's premises and of the Data Controller's property, protection of the physical safety and property of the Data Controller's employees and visitors, and investigation of the circumstances of any accidents or criminal offences that may occur.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in operating an electronic video surveillance system in order to protect its property, safeguard the physical safety of its guests, and investigate the circumstances of any criminal offences.

Scope of the data processed: The image and video recording of the natural person (hereinafter jointly: recording)

Planned deadline for data processing: For a maximum of 15 calendar days from the making of the recording, or until the data subject objects.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: Security guard

2.16 Processing related to the GDPR

Processing of data in connection with compliance with the GDPR.

Legal basis for data processing: Compliance with a legal obligation to which the Data Controller is subject (Article 6(1)(c) GDPR).

Scope of the data processed: Name, data protection identifier; the date, type, content and outcome of data subject requests; the date, documentation and outcome of incidents

Planned deadline for data processing: Not to be destroyed.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: Legal adviser, GDPR adviser

2.17 Processing of data for the purpose of legal and other claim enforcement

The Data Controller retains the personal data it processes, for the purpose of legal and other claim enforcement, for the duration of the general limitation period following the provision of the data.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in keeping records of the personal data of the data subjects with whom it has a relationship, for the duration of the general limitation period.

Scope of the data processed: Name, address, phone number, email address, IP address

Planned deadline for data processing: The last working day of January of the 4th year following the reclassification.

Source of data collection: Data already held by the Data Controller for other processing purposes

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: IT service provider, web and application service provider

2.18 Recording of the Data Controller's online workplace meetings, documenting their content, performing the Company's administrative tasks, and ensuring the continuity of work

Online meetings are recorded in video form in order to document what was said at the meeting and to ensure the continuity of work.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in recording what is said at workplace meetings in order to ensure the continuity of work, so that the outcome of the discussions is also available to those who were unable to attend the given meeting.

Scope of the data processed: The image, video recording and voice of the natural person.

Planned deadline for data processing: A maximum of 10 days.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.19 Management of subcontractors and partners; registration and tracking of the related tasks and activities

Use of a filing system.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in keeping records of the data of contact persons.

Scope of the data processed: Name, phone number, email address

Planned deadline for data processing: Until the last working day of January of the 5th year following the termination of the contract, or until the data subject objects.

Source of data collection: Data provided by the data subject, the data subject's employer, or the data subject's partner

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: SalesAutopilot

2.20 Operation of a message wall

Displaying, moderating and otherwise managing the text messages sent by visitors during events.

Legal basis for data processing: Performance of a contract (Article 6(1)(b) GDPR).

Scope of the data processed: The nickname freely chosen by the user, and the text of the message

Planned deadline for data processing: 10 seconds after the message has been displayed on the screen.

Source of data collection: Data provided by the data subject

Reclassification processing purpose:

New processing deadline:

Categories of data processors: IT operator

2.21 Handling anonymous whistleblowing reports in order to investigate the report and to remedy or put an end to the reported conduct

Where information is reported concerning an unlawful or allegedly unlawful act or omission, or other abuse, the Data Controller processes the data of the person under investigation (whose conduct or omission gave rise to the report) and of the persons who have substantive information.

Legal basis for data processing: Compliance with a legal obligation to which the Data Controller is subject (Article 6(1)(c) GDPR).

Scope of the data processed: The data, provided in the report, of the person under investigation and of the persons who have substantive information

Planned deadline for data processing: Until the investigation of the report (in the case of rejection) or until the remedying of the conduct that is the subject of the report.

Source of data collection: Data provided by the reporting person

Reclassification processing purpose: Processing of data for the purpose of legal and other claim enforcement

New processing deadline: 5 years from the date of the report

Categories of data processors: N/A

2.22 Handling named whistleblowing reports in order to investigate the report and to remedy or put an end to the reported conduct

Where information is reported concerning an unlawful or allegedly unlawful act or omission, or other abuse, the Data Controller processes the data of the reporting person, the person under investigation and the persons who have substantive information.

Legal basis for data processing: Compliance with a legal obligation to which the Data Controller is subject (Article 6(1)(c) GDPR).

Scope of the data processed: The data, provided in the report, of the reporting person, the person under investigation and the persons who have substantive information

Planned deadline for data processing: Until the investigation of the report (in the case of rejection) or until the remedying of the conduct that is the subject of the report.

Source of data collection: Data provided by the data subject and the reporting person

Reclassification processing purpose: Processing of data for the purpose of legal and other claim enforcement

New processing deadline: 5 years from the date of the report

Categories of data processors: N/A

2.23 Management of the electronic access control system

Operation of a photo-based card access control system, production of access cards, and recording of entry and exit data.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in protecting its assets and controlling access.

Scope of the data processed: Name, unique identifier, facial image

Planned deadline for data processing: Until the last day of January following the termination of the subcontractor contract, or until the data subject objects.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: Security guard, system operator, application service provider

2.24 Management of the photographs required for photo access cards

Management of the photographs required for the production and use of access cards.

Legal basis for data processing: Consent of the data subject (Article 6(1)(a) GDPR).

Scope of the data processed: Name, unique identifier, facial image

Planned deadline for data processing: Until destruction following the withdrawal of the entry authorisation, or until the withdrawal of consent.

Source of data collection: Data provided by the data subject

Reclassification processing purpose:

New processing deadline:

Categories of data processors: Security guard, system operator, application service provider

2.25 Management of the professional training and qualifications required for compliance with fire safety, occupational health and workplace safety requirements

Verification and management of the professional training, qualifications, certificates and licences of the persons performing fire safety, occupational health and workplace safety tasks.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in complying with fire safety, workplace safety and occupational health rules, and in verifying such compliance.

Scope of the data processed: Name, phone number, name of the qualification, document evidencing the qualification, certificate, licence, photo ID

Planned deadline for data processing: Until the last working day of January of the 5th year following the termination of the contract or the completion of the task, or until the data subject objects.

Source of data collection: Data provided by the data subject or by the partner

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors:

2.26 Issuing professional and complimentary tickets

The Data Controller may offer professional or complimentary tickets to the data subjects concerned.

Legal basis for data processing: Performance of a contract (Article 6(1)(b) GDPR).

Scope of the data processed: Name, email address, home address, tax identification number, details of the concert or event attended

Planned deadline for data processing: Until the last working day of January of the year following the event.

Source of data collection: Data provided by the data subject

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: IT operator

2.27 Creation of Budapest Park Staff user accounts, access management, and use of the platform

The Data Controller uses the Budapest Park Staff online platform for the purposes of organising work; managing staff schedules, applications, attendance and working-time data, absences, delays, feedback and other work-organisation information; and keeping contact with the data subjects. The Data Controller creates user accounts for the use of the Budapest Park Staff online platform, manages access rights, and ensures the identification and authentication of users. It is not possible to register on the platform independently: the Data Controller records the data subject's email address and sends an invitation, on the basis of which the data subject can complete the registration; thereafter, the data subject can access the system with the rights corresponding to their role.

Legal basis for data processing: Performance of the agency contract, subcontractor contract or other contract for the performance of work (Article 6(1)(b) GDPR).

Scope of the data processed: Name, email address, phone number, user ID, encrypted password, role, access rights, and data related to the invitation, registration, password reset and account activation.

Planned deadline for data processing: For the duration of the user access or of the data subject's legal relationship, and thereafter for the period necessary for the enforcement of legal claims.

Source of data collection: Data provided by the data subject, data recorded by the Data Controller or a person authorised by it, and data generated in the course of use.

Reclassification processing purpose: Processing of data for the purpose of legal and other claim enforcement.

New processing deadline: The last working day of January of the 4th year following the reclassification.

Categories of data processors: IT system developer and operator, hosting and server operator, email delivery service provider.

Categories of recipients: Authorities and courts.

2.28 Testing and development of the Budapest Park Staff platform

Prior to the introduction of the Budapest Park Staff platform and during its operation, the Data Controller performs tests in order to verify the operation, usability and error-free functioning of the system and its fit with the work-organisation processes, and to develop the platform.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in establishing and developing a properly functioning IT system that effectively supports work organisation.

Scope of the data processed: Name, email address, role, the operations performed during testing, error reports, observations, feedback, and the technical and activity data generated during testing.

Planned deadline for data processing: Until the closure of the testing or development and the evaluation of the results. Data processed solely for testing purposes are subsequently deleted or anonymised by the Data Controller, unless they may lawfully be further processed in live operation.

Source of data collection: Data provided by the data subject, and data generated in the course of the use of the system.

Reclassification processing purpose: N/A

New processing deadline: N/A

Categories of data processors: IT system developer and operator, hosting and server operator.

Categories of recipients:

2.29 IT security of Budapest Park Staff and logging of system use

The Data Controller logs the use of the system in order to ensure the secure operation of Budapest Park Staff, prevent unauthorised access and misuse, investigate errors and security incidents, and ensure the auditability of the operations performed in the system.

Legal basis for data processing: Legitimate interest of the Data Controller (Article 6(1)(f) GDPR). The Data Controller has a legitimate interest in ensuring the security of the IT system and of the personal data processed in it, and the auditability of the processing operations.

Scope of the data processed: User ID, IP address, login data, unsuccessful login attempts, account lockout data, the type and time of the operations performed, the previous and new state of the modified data, and the log data related to email sending and system errors.

Planned deadline for data processing: For the period necessary to ensure IT security and accountability.

Source of data collection: Data generated in the course of the use of the system.

Reclassification processing purpose: Processing of data for the purpose of legal and other claim enforcement.

New processing deadline: The last working day of January of the 4th year following the reclassification.

Categories of data processors: IT system developer and operator, hosting and server operator, IT security service provider, email delivery service provider.

Categories of recipients: Authorities and courts.

3. Consequences of failure to provide data

Possible consequence of the failure to provide data: the purpose of the processing cannot be achieved.

4. Data subjects

Natural persons — and the representatives and employees of legal persons — who assist in the provision of the Company's services and have a contractual relationship with the Company or with its contracted partners (subcontractors and their subcontractors).

5. Mandatory data

On data entry interfaces where the provision of all data is mandatory, the Data Controller does not separately mark the mandatory fields. On interfaces where not all fields are mandatory, the Data Controller marks the mandatory data fields with an asterisk (*).

6. Children

Our services are not intended for persons under the age of 18 and do not qualify as information society services. We ask that persons under the age of 18 do not provide personal data to the Data Controller. If we become aware that we have collected personal data from a child under the age of 18, we will take the necessary steps to delete the data as soon as possible. Where a minor under the age of 18 visits our events, they may enter the Company's premises under the conditions set out in the GTC.

7. Information on the use of data processors

In the course of the processing, the Data Controller transfers data to the data processor(s) contracted for the performance of the contract.

Categories of data processors: IT operators, web hosting providers, web content developer, property protection service provider, contracted call centre, hostess service provider, web service provider, social media platforms, invoicing service provider, partner event organising company, marketing agencies, legal adviser, GDPR adviser, photo and video service provider, event organiser, Google G Suite.

Categories of recipients: Courier services, freight forwarding companies, Hungarian Post, authorities, internet payment service providers, ticket sales portals.

8. Persons entitled to access the data

The Data Controller does not transfer the data to any third party other than the data processor(s) and recipients indicated in point 7.

8.1 Access to IT backup data

The Data Controller stores IT security backups separately, subject to access control. Backed-up data may be accessed only by IT operations staff, under documented procedures. For restoration from backup, the Data Controller maintains a documented procedure for reviewing the restored data before they are returned to live use.

8.2 Access to the data of the video surveillance system

The Data Controller does not transfer the recordings to any third party other than the property protection service provider indicated in point 7. The recordings may be accessed only by the designated employees of the Data Controller and of the data processor(s).

Recordings previously made by the electronic surveillance system may be accessed by the Data Protection Manager, the Head of Security, the IT Operator and the Chief Executive Officer. At the data subject's request, the data subject may access recordings of his or her own person only, and only in the presence of one of the persons listed above. Access must in all cases be requested in writing from the Data Protection Officer.

The Data Controller draws up minutes of each instance of access, which the Company retains for 1 year.

8.3 Persons entitled to restrict the images of the electronic surveillance system

Recordings made by the electronic surveillance system may be restricted only where the Data Controller has detected an event that is likely to jeopardise the purpose pursued by the electronic surveillance system.

At the data subject's request, only the processing of recordings of the data subject's own person may be restricted. The data subject must request the blocking in writing from the Data Protection Officer, indicating its purpose and expected duration.

The Data Controller draws up minutes of each step of the blocking process, which it retains for 1 year.

9. Disclosure of data

The Data Controller does not disclose the recordings of the electronic surveillance system to the public.

10. Processing of data received from third parties

Where the User/Partner provides the Data Controller with the personal data of another natural person rather than his or her own, it is the sole responsibility of the User/Partner to ensure that the data were provided with the consent, knowledge and appropriate information of that natural person. The Data Controller is not obliged to verify this. The Data Controller draws the attention of the User/Partner to the fact that if the User/Partner fails to comply with this obligation and the data subject consequently asserts a claim against the Data Controller, the Data Controller may pass the claim asserted and the amount of the related damage on to the User/Partner.

11. Data transfers to third countries or international organisations

In the case of data transfers to countries outside the EEA, the Data Controller transfers the users' data to the following recipients, as data processors, subject to the following safeguards.

Recipient in a non-EEA country	Safeguards applicable to the transfer
Google	SCC + DPA

12. Rights of data subjects

At the contact details indicated in point 1, the data subject may request from the Data Controller:

- access to a copy of his or her personal data processed by the Data Controller;
- the rectification of his or her data;
- information on the purpose and legal basis of the processing;
- the erasure of his or her personal data and the restriction of the processing.

The data subject may exercise the above rights at any time.

The data subject may also submit the following to the Data Controller at any of the contact addresses indicated in point 1:

- a request for the transmission of his or her data to another controller, provided that the processing is based on a contract or on consent and is carried out by the Organisation by automated means;

- a withdrawal of the consent previously given to the processing.

The Data Controller shall deal with or reject (stating its reasons) the request without undue delay, and in any event within 1 month of its submission — in exceptional cases within the longer period permitted by law — and shall inform the data subject of the outcome in writing.

12.1 Cost of the information

The Organisation provides the measures and the necessary information free of charge on the first occasion.

If, within one month, the data subject requests the same data for a second time and the data have not changed in the meantime, the Data Controller charges an administrative fee.

- The administrative fee is calculated on the basis of the hourly cost of the statutory minimum wage, applied as an hourly rate.
- The number of working hours spent providing the information is charged at the above hourly rate.
- In addition, in the case of a paper-based information request, the printing costs of the reply at cost price and the postage costs are charged.

12.2 Refusal of information

The Data Controller rejects the request for information if the request is manifestly unfounded, if the data subject is not entitled to the information, or if the Organisation, as data controller, can demonstrate that the data subject already has the requested information.

If the request is excessive, in particular because of its repetitive character, the Organisation may refuse to act on it where

- the data subject submits, for the third time within one month, a request concerning the same subject matter for the exercise of his or her rights under Articles 15 to 22.

12.3 Right to object

The data subject has the right to object at any time to the processing of his or her personal data based on legitimate interest or carried out in the exercise of official authority.

In that case, the Organisation may no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or which are related to the establishment, exercise or defence of legal claims.

If it finds the objection well founded, the Organisation terminates the processing — including any data transfer and further data collection — as soon as possible, and notifies everyone to whom it previously transferred the data subject's data of the objection.

Dealing with the request is free of charge, except for unfounded or excessive requests, for which the Data Controller may charge a reasonable fee corresponding to its administrative costs. If the data subject disagrees with the Data Controller's decision, he or she may bring the matter before a court.

13. Information on data security measures

The Data Controller processes the data in a closed system, in accordance with the requirements of its Information Security Policy.

The Data Controller ensures data protection by design and by default. To this end, it applies appropriate technical and organisational measures in order to:

- regulate access to the data precisely;
- grant access only to persons who need the data in order to perform their tasks, and even then only to the minimum data necessary for the performance of the given task;
- select the data processors it engages with due care, and ensure the security of the data through appropriate data processing agreements;
- ensure the integrity, authenticity and protection of the data processed.

The Data Controller applies reasonable physical, technical and organisational security measures to protect the data subjects' data, in particular against their accidental, unauthorised or unlawful destruction, loss, alteration, transfer, use, access or processing. The Data Controller notifies the data subject without delay of any known unauthorised access to or use of personal data involving a high risk to the data subject.

Where the transfer of a data subject's data is necessary, the Data Controller ensures the appropriate protection of the transferred data, for example by encrypting the data file. The Data Controller bears full responsibility for the processing of data subjects' data carried out by third parties.

The Data Controller also ensures, by means of appropriate and regular backups, that the data subjects' data are protected against destruction and loss.

14. Remedies

Any data subject who considers that

- a) the Data Controller restricts the exercise of his or her rights, or rejects a request to that effect, may initiate an investigation by the National Authority for Data Protection and Freedom of Information (NAIH) in order to examine the lawfulness of the Data Controller's action;
- b) the Data Controller infringes the legal requirements applicable to the processing of personal data in the course of processing his or her personal data,
- may request the National Authority for Data Protection and Freedom of Information to conduct data protection authority proceedings, or
- may bring an action against the Data Controller before a court; the action may, at the data subject's choice, also be brought before the regional court (törvényszék) having jurisdiction at the data subject's place of residence or place of stay.

Contact details of the National Authority for Data Protection and Freedom of Information:

President: Dr. Attila Péterfalvi

Address: 1055 Budapest, Falk Miksa utca 9-11.

Mailing address: 1363 Budapest, Pf. 9.

Phone: +36-1-3911400

E-mail: ugyfelszolgalat@naih.hu

www.naih.hu

Budapest, 23/07/2026