**GENERAL PRIVACY POLICY**

**OF MULTIAPPSFACTORY KFT.**

**MultiAppsFactory Kft., a company providing an online radio media content aggregator service** on the myradiostanice.rs website (hereinafter referred to as “Website”) and the iOS, Android and television applications of MyRadioStanice (hereinafter referred to as “Application”), **as controller** (hereinafter referred to as “Controller”, “we”), **hereby informs the data subjects** (visitors and users of the Website and the Application, as well as the contact persons of our business partners interested in our services and using our services) that, **while respecting the data subjects’ moral rights and right to informational self-determination, it shall act in accordance with the provisions of this General Privacy Policy** (hereinafter referred to as “Privacy Policy”, “Policy”) **during its processing activity**.

1. **GENERAL INFORMATION ON PROCESSING**
2. **WHAT IS DATA PROTECTION AND WHY IS IT IMPORTANT?**

Data protection is an important means of protecting privacy.

It aims to protect the rights of the data subjects and to prevent personal data from being disclosed to unauthorised persons.

The principles, rules and procedures that ensure the lawful processing of personal data and the protection of the data subjects do not in fact protect the data, but the owner of the data.

1. **OUR COMMITMENT TO THE PROTECTION OF PERSONAL DATA**

In the course of its business activities, the Controller processes the personal data of

* visitors and users of the Website,
* users of the Application
* those interested in our services,
* contact persons of the online radio stations that use our service (hereinafter referred to as “Online Radio Station”).

(hereinafter referred to as “Data Subject”, “Data Subjects”, “You”).

In this Privacy Policy, and wherever your personal data is used, **we provide concise, specific and transparent information** about the way, purposes and circumstances of the processing.

In all cases, we process the personal data provided to us in compliance with the applicable Hungarian and European Union data protection legislation and jurisprudence, and we take the technical and organisational measures necessary **for** proper and **secure processing**.

We respect the principle of **accountability** by providing up-to-date and easily understandable information about our processing activities.

We reserve the right to update this Privacy Policy on an ongoing basis in light of changes in legislation and the continuous development of jurisprudence and changes to the services we offer.

You can access the current version of the Privacy Policy, as well as previously applicable versions, at https://myradiostanice.rs/public/docs/privacy-policy/sr\_RS/.

1. **DEFINITIONS**

Knowledge of the basic concepts of data protection is essential to understand this Policy. Definitions are set out in Article 4 of the GDPR[[1]](#footnote-1), from which we highlight the following:

**“personal data”**: any information relating to an identified or identifiable natural person (‘data subject’);

**“identifiable”**: a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors, is identifiable;

**“sensitive data”:** any data that fall within special categories of personal data, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons.

**“processing”:** any operation or set of operations which is performed on personal data;

**“processing operations”:** any collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

**“disclosure”:** making the data available to anyone;

**“erasure”:** rendering data unrecognisable in such a way that it is no longer possible to recover it;

**“filing system”**: any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

**“restriction of processing”**: the marking of stored personal data with the aim of restricting their processing in the future;

**“profiling”**: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

**“pseudonymisation”**: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

**“controller”:** the person who, alone or jointly with others, determines the purposes and means of the processing;

**“processor”:** a person who processes personal data on behalf of the controller;

**“data subject”**: any specified natural person who is identified or identifiable, directly or indirectly, on the basis of personal data;

**“recipient”:** to whom the personal data is disclosed (whether a third party or not);

**“third party”:** anyone other than the data subject, the controller, the processors or those acting on their behalf;

**“consent of the data subject”:** any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them;

**“personal data breach”**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transferred, stored or otherwise processed;

**“newsletter”**: an electronic letter, transactional, promotional or other campaign information, typically generated automatically and sent by an application, sent to the email address of persons subscribed to a mailing list;

**“Facebook pixel (Facebook cookie)”:** the Facebook pixel is a code that allows the Website to report conversions, create target audiences and provide the Website owner with detailed analytics data about visitors’ use of the Website. The Facebook remarketing pixel tracking code allows personalised offers and ads to be displayed to the visitors of the Website on Facebook. The Facebook remarketing list is not suitable for personal identification (fr, tr).

More information about the Facebook Pixel is available here:<https://www.facebook.com/business/help/651294705016616>

**“adblock”:** Adblock Plus blocks all annoying ads on the Internet by default, including video ads on YouTube, Facebook ads, flashy ad bars, pop-ups, pop-up screens and more. This is possible based on the selected filter list (k). Simply [install the Adblock Plus software](https://adblockplus.org/) and, if you wish, you can customise it to suit your specific browsing needs.

1. **PURPOSE OF THE PRIVACY POLICY**

The purpose of this Policy is to

* ensure that data subjects can easily see and understand
	+ the way we collect your personal data on the Website and in the Application, the purpose for which we use them and the principles and rules according to which we process them,
	+ what personal data is processed in the course of providing the prominent position and premium partner service for Online Radio Stations (hereinafter referred to as “Services Provided to Online Radio Stations”) and the basic and premium services provided to Users (hereinafter referred to as “Services Provided to Users”) (“Services Provided to Online Radio Stations” and “Services Provided to Users” collectively referred to as “Services”),
	+ under what circumstances we may disclose your personal data to others and
	+ what rights you have in relation to the processing of your personal data.
1. **THE PERSONAL SCOPE AND SUBJECT MATTER OF THE GENERAL PRIVACY POLICY**

The personal scope of this Policy applies to visitors interested in the Services provided by the Controller and available on the Website, users and Online Radio Stations using the Services, the contact persons of the Controller’s contractual partners, the Controller and the Processors.

In this Policy, the Controller provides detailed information on the material circumstances, methods, principles, legal basis, purposes and duration of processing in relation to its Services.

1. **PRINCIPLES OF PROCESSING**

| **DATA PROTECTION PRINCIPLE** | **CONTENT** |
| --- | --- |
| * 1. **Legality, fairness and transparency**
 | The processing must be lawful, fair and transparent throughout the period of processing.  |
| * 1. **Purpose limitation**
 | The principle of purpose limitation means that we can only process your personal data for clearly defined, legitimate purposes and that the collection of data and other processing operations must be compatible with the purposes of the processing. It follows from the principle of purpose limitation that personal data can only be processed until the purpose of the processing is achieved.  |
| * 1. **Data minimisation principle**
 | The principle of data minimisation means that only personal data that are strictly necessary for the purposes for which they are processed may be lawfully processed. |
| * 1. **Accuracy**
 | The principle of accuracy means that the data stored in our filing systems must be true and correct throughout the entire processing process. If the data is inaccurate or incorrect, we shall cooperate with you to restore the accuracy of your personal data based on your request. |
| * 1. **Storage limitation**
 | The principle of storage limitation means that the personal data can only be stored until the purpose of the processing is achieved. Personal data cannot be cumulated or stored indefinitely. To comply with this principle, we determine the duration of the processing or, where this is not possible, the criteria for determining the duration.  |
| * 1. **Integrity and confidentiality**
 | As a controller, we treat personal data provided to us as confidential. Your personal data may only be accessed by our employees and agents who are authorised to process your personal data on the basis of their job or function. We ensure that documents containing personal data and data are kept in accordance with the state of the art and with the technical and organisational security measures expected of similar organisations. |
| * 1. **Accountability principle**
 | The principle of accountability means that as a controller, we must be able to demonstrate the lawfulness of processing, i.e. compliance with the GDPR. In order to ensure accountability, we document our processing activities in accordance with the GDPR. We keep records of the provision and publication of the necessary information, our data processing activities, our data security measures, personal data breaches and data protection-related enquiries.  |

1. **WHAT PERSONAL DATA MAY WE PROCESS ABOUT YOU?**

We may collect the following personal information about you depending on how you use our Website and Application and the information you share with us when you enquire about or use our Services:

* 1. name (surname and/or first name)
	2. email address
	3. home or billing address (country, city, postcode, house number)
	4. tax number (only in case of invoice requests)
	5. phone number (business or personal)
	6. username
	7. password provided during registration
	8. any other personal information that you share with us when you fill in the contact form
	9. the personal information and opinions that you share with us when completing a test or survey and when recommending our services on our website
	10. IP address, password, login details (e.g. date of registration), cookies and other technical information that may tell us how you use our website
	11. job title and name of employer
	12. the personal information you provide in the course of the complaint handling process.
1. **WHAT DO WE USE YOUR PERSONAL DATA FOR?**
	1. You can enquire about our services by filling in our contact form.
	2. In line with the principle of accountability, we automatically log technical data and conversion events of users of the Website which are generated while using the Services in order to ensure technical and security requirements, based on our legitimate interest.
	3. We use the contact details of our business partners in connection with the creation, performance and termination of contracts, for the purpose of offering additional Services related to the Services used and for the purpose of fulfilling our accounting obligations.
	4. We process the data of the persons designated as contact persons for the purposes of creating, performing, amending and terminating the contract.
	5. Your personal data is also required to identify and contact you in order to carry out the complaint procedure on the basis of your complaint.

We use your personal data collected through the use of cookies and social media pixels for the following purposes:

In order to operate, facilitate and secure the use of the Website, to track and analyse user activity on the Website and to display relevant advertising, we use cookies, most of which cannot be used for identification purposes in the absence of further information, but some of which may contain a cookie identifier that can be used for individual identification. You can read more about this in the **Cookie Policy**.

Social media pixels, as software codes, enable the automated collection, transmission and evaluation of your personal data during your visit to the Website for the purpose of relevant advertising and remarketing activities for the social media provider. We cannot link this data to your person. Details are also **provided in the Cookie Policy**.

1. **ON WHAT LEGAL BASIS DO WE PROCESS YOUR PERSONAL DATA?**

We may process personal data of data subjects on the following legal bases under the GDPR:

* the **Data Subject has given their consent** to the processing of their personal data for one or more specific purposes;
* the processing is necessary for **the performance of a contract** to which the Data Subject is a party or for taking steps at the request of the Data Subject prior to entering into the contract;
* processing is necessary **for compliance with a legal obligation** to which the Controller is subject;
* the processing is necessary for the purposes of the **legitimate interests** pursued by the Controller or a third party and the Controller has established, by means of an interest balancing test, that the interests or fundamental rights and freedoms of the Data Subject, which require the protection of personal data, do not override those interests.

1. **DETAILED INFORMATION ON EACH PROCESSING OPERATION**
	* + 1. **PROCESSING OPERATIONS CONCERNING USERS**

* 1. **PERSONAL DATA PROCESSED FOR THE PURPOSE OF CONTACTING THE CONTROLLER**

**Data subjects:** users of the Website who wish to contact the Controller by filling in the contact form

**Personal data processed:** name, email address, personal data that may appear in the subject and text of the message

**Source of data:** it is directly the data subject in respect of the name and email address, and it is the user in respect of personal data which may be contained in the subject and text of the message, who must obtain the data subject’s consent

**Purpose of processing**: identification, maintaining contact, answering the user’s queries and questions, providing assistance related to the use of the service

**Legal basis for processing**: voluntary consent of the data subject pursuant to Article 6(1)(a) of the GDPR

**Duration of processing:** until the data subject’s consent is withdrawn, but for a maximum period of six months

**Possible consequences of failure to provide data:** in the absence of personal data, it is not possible to identify or contact the data subject

**Whether data is transferred:** no, except for processors providing IT services and hosting services

* 1. **PERSONAL DATA PROCESSED FOR THE PURPOSE OF CONTACTING ONLINE RADIO STATIONS**

**Data subjects:** users of the Website who wish to contact the Online Radio Station by filling in the contact form

**Personal data processed:** name, email address, personal data that may appear in the subject and text of the message

**Source of data:** it is directly the data subject in respect of the name and email address, and it is the user in respect of personal data which may be contained in the subject and text of the message, who must obtain the data subject’s consent.

**Purpose of processing**: On the basis of an agreement with the Online Radio Station, the Controller allows you to contact the Online Radio Station on the Website via the contact form available in the Hyperlink Directory of the Website, using the email address available on the Online Radio Station’s own website. With regard to the personal data provided in the contact form, the Controller and the Online Radio Station are considered as separate controllers, as they process the personal data for different purposes. The sole purpose of the Controller’s data processing is to be able to exclude potentially spamming or harassing users from using the site, and to report the error to the user in case of an email sending error.

**Legal basis for processing**: voluntary consent of the data subject pursuant to Article 6(1)(a) of the GDPR

**Duration of processing:** until the data subject’s consent is withdrawn, but for a maximum period of six months

**Possible consequences of failure to provide data:** in the absence of data provision, the Controller is unable to filter out spamming users and cannot control that a user cannot submit more than three contact forms in a day

**Whether data is transferred:** no, except for processors providing IT services and hosting services

* 1. **IMAGES AND VIDEOS DISPLAYED ON THE CONTROLLER’S FACEBOOK PAGE**

**Data subjects:** data subjects in photos related to news stories about public figures and funny pictures used on the Controller’s Facebook page

**Personal data processed:** name, image, video, audio

**Source of data:** third party

**Purpose of processing**: to inform and entertain the followers and visitors of the Controller’s Facebook page

**Legal basis for processing**: journalistic processing, the legitimate interest of the Controller in informing and entertaining users when editing the content of the Facebook page pursuant to Article 6(1)(f) of the GDPR

**Duration of processing:** until the given content is removed from our Facebook page

**Possible consequences of failure to provide data:** in the absence of data provision, the Controller cannot publish informative and entertainment content containing the image of the data subject on the Controller’s Facebook page for users.

**Whether data is transferred:** no, except for Meta Platforms Ireland Ltd, which operates the Facebook service

* 1. **PUBLISHING COMMENTS USING THE FACEBOOK COMMENT PLUGIN EMBEDDED IN THE WEBSITE**

**Data subjects:** users who can comment on the content of the Website through their Facebook account and share their comments with their Facebook friends

**Personal data processed:** Facebook profile (name, picture), personal data that may appear in comments

**Source of data:** the Data Subject via an external service provider

**Purpose of processing**: to display comments on articles published on the Website

**Legal basis for processing**: the publication may take place after the data subject has logged in to Facebook and given their consent on the basis of the Facebook privacy information enabling this embedding

**Duration of processing:** until the Data Subject removes the post by themselves or until the deletion of the given content from our website

**Whether data is transferred:** no, except for Meta Platforms Ireland Ltd, which operates the Facebook service

* 1. **PROCESSING RELATED TO THE AUDIENCE MEASUREMENT OF ONLINE RADIO STATIONS**

**Data subjects:** subscribers to the Premium Service of the Controller

**Personal data processed:** the subscriber’s own identifier, to which a record, a listening time (TIME) and the radio’s identifier (RID) will be assigned while the subscriber is listening to Online Radio Stations, which measures how long the subscriber listens to which Online Radio

**Source of data:** the Data Subject

**Purpose of processing**: the legitimate interest of the Controller to be able to account for the revenue share based on the audience data under its contract with the Online Radio for the Premium Partner Service

**Legal basis for processing**: legitimate interest of the Controller pursuant to Article 6(1)(f) of the GDPR

**Duration of processing:** until the payment obligation is fulfilled on the basis of the settlement of accounts with the Online Radio Station for the given year

**Whether data is transferred:** if requested by the Online Radio Station, it can access the audience measurement

**f. PROCESSING IN CONNECTION WITH THE EMBEDDING OF ONLINE RADIO STATIONS IN THE WEBSITE**

**Data subjects:** users of the Website

**Personal data processed:** the user’s IP address, browser information or other personal data stored in the cookies used by the Online Radio Station embedded in the Website

**Source of data:** the Data Subject via an external service provider

**Purpose of processing**: in accordance with the processing purpose of the cookies embedded in the Website, as set out in the cookie management platform and the Cookie Policy

**Legal basis for processing**: in the case of audience measurement cookies, the legitimate interest of the Controller as defined in Article 6(1)(f) of the GDPR, in the case of other cookies, the data subject’s consent as defined in Article 6(1)(a) of the GDPR

**Duration of processing:** varies according to the cookies as set out in the Cookie Management Platform or Cookie Policy

**Whether data is transferred:** in the case of third party cookies, the personal data stored in the cookies is transferred to the third party service provider that placed the cookie

**2. WEB SERVER LOGGING**

**Data subjects:** users of the Website whose user activity is automatically logged by the web server

**Personal data processed:** identification number, date and time of visit, address of the page visited and the time spent on it, IP address of the user’s computer, type and version of their operating system and browser, and the user’s searches

**Source of data:** the Data Subject

**Purpose of processing**: during the visit to the Website, the Controller records the data of the visitors in order to monitor the operation of the Services and the functions of the Website and to prevent abuse.

**Legal basis for processing:** the Controller has a legitimate interest in identifying users and preventing abuse [Article 6(1)(f) GDPR]

**Duration of processing:** one month

**Possible consequences of failure to provide data:** it is not possible to monitor the operation of the Services and the functions of the Website, or to prevent abuse in the absence of the processed visitor data. The Data Subject may not object to the recording of data, because the processing is justified by compelling legitimate grounds (currently widely used technical solutions) without which the Service cannot be provided.

**Whether data will be transferred:** no, except for data processors providing IT services, hosting services

**3. DATA OF ONLINE RADIO STATIONS, BUSINESS PARTNERS**

**Data subjects:** private individual users of the Controller’s Services

**Personal data processed:** surname, first name, address, content of the record, name, address and tax number in the case of VAT invoices, name, quantity, purchase price of the service used, method of payment, other personal circumstances relating to the use of the service, data on business card

**Source of data:** the data subject directly

**Purpose of processing**: use of the services of the Controller, maintaining contact, registration of partners, distinguishing them from each other, use of the Service, fulfilment of payment obligation, billing

**Legal basis for processing:** processing is necessary for the performance of the contract [Article 6(1)(b) GDPR], in the case of billing data, Article 6(1)(c) GDPR, (processing is necessary for the performance of a legal obligation to which the Controller is subject, with regard to Section 169(2) of the Accounting Act).

**Duration of processing:** 5 years after termination of the contract in the case of a contract, 8 years for billing data in accordance with Section 169(2) of the Accounting Act, or 6 months after contact in the absence of a contract

**Possible consequences of failure to provide data:** it is not possible to conclude a contract or to fulfil the payment obligation and issue invoices without the personal data processed.

**Whether data will be transferred:** no, except for data processors providing IT services, hosting services

**4. CONTACT PERSONS OF ONLINE RADIO STATIONS, BUSINESSES CONTRACTING WITH THE CONTROLLER**

**Data subjects:** employees of third parties (Online Radio Stations, other companies) or persons who have other employment-related relationships with them, designated as contact persons in the performance of the contract

**Personal data processed:** surname, first name, email address, phone number, job title, other data on business card

**Source of data:** the Controller’s contractual partner

**Purpose of processing**: maintaining contact, fulfilling rights and obligations arising from the contract.

**Legal basis for processing**: legitimate interest in facilitating cooperation between the parties and communication between the parties for the conclusion, performance and termination of the contract, pursuant to Article 6(1)(b) of the GDPR

(Interest balancing test available on request.)

**Duration of data processing:**until the termination of the business relationship with the contractual partner or a change in the contact person of the contractual partner. **Whether data will be transferred:** no, except for data processors providing IT services, hosting services

**5. PROCESSING IN RELATION TO PERSONS PARTICIPATING UNDER AN EMPLOYMENT-RELATED RELATIONSHIP**

**Data subjects:** natural persons who have a personal service or works relationship with the Controller

**Processed personal data:** name, address, email address, mother’s name, place and date of birth, tax identification number, tax number, contact details, identity document, passport number, bank account number of the natural person vicarious agents (suppliers) contracting with the Controller

**Source of data:** the Data Subject

**Purpose of data processing**: conclusion, performance and termination of the contract between the Controller and the data subject, fulfilment of the legal obligation to retain tax documents and accounting records, enforcement of claims, and in the event of a dispute, the ability to prove the content of the contractual relationship

**Legal basis for processing**: In the context of registering the contracting party’s data, the legal basis for processing is the performance of the contract pursuant to Article 6(1)(b) of the GDPR

In the context of issuing and keeping accounting records, the legal basis for processing is the fulfilment of a legal obligation to which the Controller is subject pursuant to Article 6(1)(c) of the GDPR.

**Duration of data processing:** **The fulfilment of the Controller’s statutory obligation under Section 169 of Act C of 2000 on Accounting (hereinafter referred to as “Accounting Act”) to keep accounting records for 8 (eight) years after the termination of the Contract, or in the event of a dispute, for 5 (five) years after the conclusion of the dispute, if later**

**Whether data will be transferred:** no, except for processors

**6. COMPLAINT HANDLING**

**Data subjects:** users who have submitted complaints about the Service

**Personal data processed:** surname, first name, email address, phone number, billing name, address, tax number

**Source of data:** the data subject

**Purpose of processing**: maintaining contact, identification, handling complaints and problems related to the ordered service.

**Legal basis for processing**: pursuant to Article 6(1)(c) of the GDPR, the legal basis for processing is the fulfilment of the controller’s obligation under Section 17/A(7) of Act CLV of 1997 on Consumer Protection, according to which  the undertaking must keep the record of the complaint and a copy of the reply for three years and present it to the supervisory authorities at their request.

**Duration of data processing:** Copies of the record, transcript of the complaint and the reply to the complaint shall be kept for 3 years pursuant to Section 17/A(7) of Act CLV of 1997 on Consumer Protection.

**Whether data will be transferred:** no, except for processors

1. **PROVISIONS ON PROCESSING RELATING TO MINORS**

Consent to processing on behalf of a **minor under the age of 14 and a data subject who is otherwise incapacitated** may be given by the legal representative.

**A minor over the age of 14 and a data subject who is otherwise of limited capacity** may give consent to processing with the consent or subsequent consent of their legal representative.

The Controller offers its Services to persons over 18 years of age, but it is not in a position to verify the eligibility of the person giving consent or to know the content of the declaration of the legal representative; therefore, the data subject or their legal representative shall guarantee that the consent is in compliance with the law. The Controller shall consider the consent of the legal representative to be granted if the Service is used.

1. **WHO WILL BE AUTHORISED TO PROCESS YOUR PERSONAL DATA?**

We, as a controller, determine the purposes and means of the processing of your personal data.

**CONTROLLER’S DATA:**

Company name: MultiAppsFactory Korlátolt Felelősségű Társaság

Registered seat: H-1024 Budapest, Margit krt. 57. 2. em. 5.

Tax number: 26278823-2-41

Company registration number: 01-09-357239

Email address: info@multiappsfactory.hu

Phone: +36-30/813-2598

As a controller, we treat personal data provided to us as confidential. Your personal data may only be accessed by our employees and agents who are authorised to process your personal data on the basis of their job or function.

1. **WITH WHOM CAN WE SHARE YOUR PERSONAL DATA?**

**PROCESSORS**

To provide the Services, we must also use the services of IT (e.g. hosting, IT services, web development) and other technical service providers.

The processors shall process your personal data on our behalf, strictly according to our instructions and with appropriate safeguards.

We also share or may share your personal data:

personal

* with our accountant to fulfil the company’s bookkeeping and accounting obligations,
* with our auditors, lawyers and other advisers when we ask them for professional advice.

**JOINT PROCESSING**

With regard to embedded content, in connection with the collection and transmission of personal data through pixels by external service providers (Meta Platforms Ireland Ltd, Online Radio Stations), the Controller and the social media service provider are joint controllers.

For more information about the pixels used on this website, please read the Cookie Policy.

**EXTERNAL SERVICE PROVIDERS**

The Controller uses external service providers in connection with the provision of the Services in a number of cases, and cooperates with such external service providers.

The personal data processed in the systems of external service providers is governed by the privacy policy of the external service provider. The Controller shall use its best endeavours to ensure that the external service provider processes the personal data transferred to it in accordance with the law and uses them only for the purposes specified by the data subject or set out in this Policy.

The Controller informs Users about the transmission of data to external service providers within the framework of this policy.

1. **HOW LONG CAN WE PROCESS YOUR PERSONAL DATA?**

Your data on the contact form shall be processed until you withdraw your consent (but for a maximum of 6 months).

If you use our Services or a contract is concluded between us, we shall process your personal data processed on the basis of the contract concluded between us for the purpose of fulfilling the contractual obligation until the expiry of the limitation period of 5 years after the termination of the contract in accordance with the Civil Code.

In case of using the Service or in case of a contractual relationship, your billing data shall be stored by the Processor we have engaged for a maximum period of 8 years, after which the data shall be deleted.

In the case of our posts containing personal data on our Facebook page, we process the data until the content is deleted from our Facebook page or, in the case of comments posted using Facebook modules embedded in our page, until the post is removed by the data subject or the content is deleted from our website.

In the case of processing in connection with complaint handling, copies of the record, transcript of complaint and reply to the complaint shall be kept for 3 years pursuant to Section 17/A(7) of Act CLV of 1997 on Consumer Protection.

## **THE IDENTITY OF EACH PROCESSOR**

Some of the personal data you provide to us may be transferred to processors we have engaged, with regard to the purposes of the processing. Processors shall process the personal data received in accordance with the terms of the data processing contract with the controllers and may not use it for any other processing purposes.

Our permanent collaborating processors are the following:

|  |  |  |
| --- | --- | --- |
| **DATA PROCESSING ACTIVITIES** | **NAME** | **ADDRESS, CONTACT DETAILS** |
| **IT operations, administrator services** | Balance 2000 Kft. | Address: H-2230 Gyömrő, Szent István út 21Website: https://balance2000.hu/Email: sales@balance2000.hu |
| **Hosting service** | Rackforest Informatikai Kereskedelmi és Szolgáltató Kft. | Address: H-1132 Budapest, Victor Hugo utca 18-22. 3. em. 3008.Website: www. rackforest.com Email: info@rackforest.hu |
| **Accounting and payroll services** | Forgóeszköz Kft. | Address: H-1083 Solymár, Orgona utca 7.Email:  |
| **Invoicing, automatic invoicing** |  Billingo Technologies Ltd. / billingo.hu | Address: H-1133 Budapest, Árbóc utca 6. I. emeletWebsite: https//www.billingo.huEmail: hello@billingo.hu |

**GENERAL TERMS AND CONDITIONS FOR DATA PROCESSING**

**In compliance with the GDPR, the processor undertakes to:**

a) process the personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or
Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing;

b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,
the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:

(i) the pseudonymisation and encryption of personal data

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(iii) the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident; and

(iv) a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures implemented to guarantee the security of the processing.

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transferred, stored or otherwise processed.

d) take measures to ensure that any natural person acting under the authority of the Processor, who has access to personal data, shall process those data exclusively on instructions from the Controller;

e) the Controller authorises the Processor to use an additional data processor in advance by means of this processing contract;

f) where the Processor uses the Services of another processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in this Processing Contract or other legal act shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing shall meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor’s obligations;

g) taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Controller’s obligation to respond to requests for exercising the Data Subject’s rights laid down in Chapter III of the GDPR;

h) assist the Controller in ensuring compliance with the obligations pursuant to Articles 32–36 of the GDPR (Security of processing, Notification of a personal data breach to the supervisory authority, Informing the data subject of the personal data breach, Data Protection Impact Assessment, Prior consultation), taking into account the nature of processing and the information available to the Processor;

i) at the choice of the Controller, delete or return all the personal data to the Controller after the end of the provision of the data processing service, and delete existing copies unless Union or Member State law requires storage of the personal data;

j) make available to the Controller any information necessary to justify the deletion of the data or copies and enable and facilitate audits, including on-site inspections, carried out by the Controller or by another auditor mandated by the Controller. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

k) notify the Controller of the data breach within 72 hours of becoming aware of it. The aforementioned notification shall at least:

(i) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data concerned by the personal data breach;

(ii) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(iii) describe the likely consequences of the personal data breach; and

(iv) describe the measures taken or proposed to be taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

l) assist the Controller in complying with the requests of Data Subjects to exercise one or more of their rights under the GDPR;

m) where the Processor receives a request from any Data Subject to exercise one or more of the rights provided for in the GDPR, the Processor shall inform the Data Subject to address the request directly to the Controller and shall inform the Controller of the request without delay;

n) keep all records required under Article 30(2) of the GDPR and, where the processing of personal data on behalf of the Controller so permits, make those records available to the Controller upon request.

The Processor undertakes to process the personal data that it processes only in accordance with the applicable law.

The Controller is entitled to check the performance of the activities set out in this contract, in particular the way in which the Data Subjects’ personal data are stored and processed, once a year at a date agreed in advance.

If the Processor suffers damage in connection with the Controller’s activities, the Controller shall compensate the Processor for such damage. If a claim for damages or proceedings are brought against the Processor in connection with the Controller’s activities, the Controller shall indemnify the Processor against any damages, fines or penalties imposed within 30 days.

1. **EXTERNAL SERVICE PROVIDERS**

**A. Service providers operating web stores for applications**

The service providers (e.g. Apple Inc., Google Inc.) that operate mobile app stores (e.g. Apple Store, Android Store) process the data of users of services installed on the end user’s device and send update notifications independently of us.

**B. External intermediary service providers**

1. When you use the Services, certain service providers (e.g. Google Inc., Twitter Inc., Facebook Inc., Pinterest Inc and Pinterest Europe Ltd., LinkedIn Corp.) provide registration and login facilitation applications in accordance with their own privacy guidelines.

With respect to content made available through the Services and shared on various social media sites, the service provider that enables the sharing of content is the controller of personal data and is subject to its own terms of use and privacy policy. Such external intermediary services are

|  |  |  |
| --- | --- | --- |
| **EXTERNAL SERVICE PROVIDERS** | **LINK TO PRIVACY NOTICE** | **LINK TO TERMS OF USE** |
| **Facebook** | <http://www.facebook.com/full_data_use_policy><https://www.facebook.com/policy/cookies/> | <http://www.facebook.com/legal/terms?ref=pf> |
| **Google**  | [https://www.google.com/intl/sr/+/policy/](https://www.google.com/intl/hu/%2B/policy/) | [https://www.google.com/intl/sr/+/policy/pagesterm.htm](https://www.google.com/intl/hu/%2B/policy/pagesterm.htm) |
| **Twitter**  | <http://twitter.com/privacy><https://help.twitter.com/en/rules-and-policies/twitter-cookies> | <http://twitter.com/tos> |

1. **Social media platforms**

Data processing on social media platforms (e.g. Facebook page) is always subject to the respective social media site’s own data processing information, rules and practices, which are continuously published on the platforms operated by the respective service provider. The social media platform and the Controller are considered as joint controllers.

Our website has share buttons that you can click to share content from our websites on social media channels such as Facebook. These buttons are not used to share your personal data with social media providers. When you click on a share button, the social media provider concerned will collect personal data directly from you. Please read the privacy statements of the social media providers with which you intend to share content before clicking on the appropriate share button.

To use the “Like” and “Comment” social plugins, the user must be logged in to their Facebook account and have consented to the placement of “Application and website cookies”. If both requirements are met, the user can see and use extensions such as the “Like” or “Comment” button. If any of the above requirements are not met, the user will not see the plugins.

**C. External web analytics and ad serving companies**

We use the services of external web analytics and ad serving companies to operate our web-based services.

In addition to cookies, web analytics and ad serving service providers use measurement pixels and campaign codes to identify advertising campaigns in order to collect information in connection with user behaviour and ad serving.

## **Google Analytics**

On our website, we use Google Analytics, an audience measurement service provided by Google Ireland Limited (Gordon House, Barrow Street, Dublin 4, Ireland), which uses cookies to analyse user behaviour. Google Analytics also records the IP address of visitors to the website, but shortens it before storing or analysing it, thereby anonymising it (where technically possible). The anonymisation takes place within the European Union or the European Economic Area. Only in exceptional cases will the full IP address be transferred to a Google server in the United States for shortening.

Google relies on the following adequacy decisions in certain cases when transferring data outside the EEA:

* [Adequacy decisions of the European Commission;](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries)
* [Adequacy decisions of the UK;](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#adequacy)
* [Adequacy decisions of Switzerland.](https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html)

Google will not merge the IP address transmitted by your browser with any other data in connection with Google Analytics. When you visit our Website, Google may combine information about your activities on our website with information about your activities on other websites using our advertising services.

Google Analytics collects information per your measurement-code configuration, as well as Google advertising cookies that are present.

In addition to reporting on site usage statistics, Google Analytics, along with some of the advertising cookies described above, can also be used to display more relevant ads in Google products (such as Google Search) and across the web.

Google Signals is a new data collection function of Google Analytics, introduced to enhance the effectiveness of remarketing and reporting, which is suitable for tracking users who have consented to “Ads Personalisation” in their personal account with Google. Google Analytics tracks the sessions and device types of all users who have logged into their Google Account and converted. Once the function is activated, Google Analytics can recognise the device from which the first click was made, other devices from which different clicks are made during the customer journey, and finally the device that leads to the conversion.

Google provides information on the display of personalised ads, the related processing operations and disabling the function at the following address: [https://support.google.com/ads/answer/2662856?hl=sr](https://support.google.com/ads/answer/2662856?hl=hu%20)

## **Google Ads, Google Adsense, Google Admob**

When you visit our Website, your web browser automatically sends certain information to Google. This includes the URL of our website and your IP address. Google can also set cookies in your browser or scan cookies that are already there. Apps that use Google’s advertising services also share additional information with Google, such as the name of the app and the unique identifier of the ads.

Google uses the information shared by websites and applications to provide, maintain and improve its services, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalise the content and ads on Google and our partners’ websites.

On our Website, we also use conversion tracking cookies to allow Google Ads to provide us with conversion statistics about the effectiveness of our ads. This is how we get information about how many people clicked on our ad and from there to our website with a conversion tracking tag. In doing so, we do not obtain any information that could identify any user.

When someone visits our site, the visitor’s cookie ID is added to the remarketing list. Google uses cookies—such as NID and SID cookies—to personalise the ads you see in Google products, such as Google Search. Such cookies are used, for example, to remember your recent searches, your previous interactions with certain advertisers’ ads or search results, and your visits to advertisers’ websites. The Ads conversion tracking feature uses cookies. Cookies are saved on the user’s computer when they click on an ad to track ad sales and other conversions. Some common uses of cookies include: selecting ads based on what is relevant to a particular user, improving campaign performance reporting, and avoiding displaying ads that the user has already viewed.

Google AdSense is an online advertising service operated by Google Inc., whose primary purpose is to sell advertising space on the Internet. The service allows website owners to register and allow text, image and video ads on their website.

As part of Google AdSense and Google Ads remarketing, Google Inc. places visitor-tracking cookies on users’ devices that track visitors’ online behaviour and allow Google Inc. to serve them advertising on the Website based on their behaviour and interests. The tracking cookie also allows Google Inc. to identify the website visitor on other websites.

The “Privacy Policy” of Google Inc. is available on the [http://www.google.hu/intl/sr/policies/privacy/](http://www.google.hu/intl/hu/policies/privacy/) website.
More useful information on the data-related activities of Google Inc., the disabling of cookies, and the personalisation of ads is available on the website of Google Inc: <https://adssettings.google.com/anonymous>

Other information is available on the following pages of Google:

Google Adsense  [https://policies.google.com/privacy?hl=sr](https://policies.google.com/privacy?hl=hu)

Google Analytics <https://developers.google.com/analytics/devguides/collection/gtagjs/cookie-usage>

Google Ads  <https://www.google.com/intl/en/policies/privacy>

If you do not wish to participate in conversion tracking, you can opt-out by disabling the option to install cookies in your browser. You will then not be included in our conversion tracking statistics.

**Social media pixels**

We use a Facebook pixel on our Website, which allows Facebook to treat visitors to our website as a target group to display Facebook ads so that certain remarketing Facebook ads are only shown to Facebook users who have shown an interest in our services.

The Facebook pixel also allows us to analyse the effectiveness of our Facebook ads for statistical and market research purposes. This will tell us whether users came to our site by clicking on the Facebook ad.

By embedding the Facebook pixel in our website, we have enabled Facebook to place a cookie on your device.

If you later log in to Facebook or visit Facebook pages while logged in, Facebook will register your visit to our website in your profile. The information we collect about you is anonymous to us, which means we cannot use it to identify you. However, your data is stored and processed by Facebook, so it can be linked to your user profile.

In the use of Facebook pixels, the Controller (we) and Facebook are considered to be joint controllers.

Facebook’s data processing is governed by its own privacy policy, so for more information about how the remarketing pixel works and how Facebook ads are displayed in general, please consult the Facebook Privacy Policy at the following link: <https://www.facebook.com/policy.php>

In the Facebook interface below, you have the option to disable data recording by the Facebook pixel and the use of your data for the purpose of displaying Facebook ads :

<http://www.youronlinechoices.com/>.

The settings are platform independent, i.e. they apply to both desktop computers and mobile devices .

The Google pixel on the Website is used to send Google Analytics data about the visitor’s device and behaviour by tracking the visitor across devices and marketing channels.

For more information on the use of cookies and social media pixels, please see our Cookie Policy, which you can access by clicking here.

**III. DATA SECURITY MEASURES**

In order to ensure the security of personal data in our processing, we take all technical and organisational measures and establish the procedural rules necessary to enforce data security standards in compliance with our obligations under the GDPR and the Privacy Act.

We ensure the security of processing by technical, organisation and organisational measures that provide a level of protection appropriate to the risks associated with the processing.

In the course of data processing we maintain

a) confidentiality, i.e. we protect the information so that only those who are entitled to it have access to it;

b) integrity, i.e. we protect the accuracy and completeness of the information and the method of processing;

c) availability, i.e. we make sure that when an authorised user needs it, they can actually access the information and the means to do so are available.

The personal data we process is treated as confidential and appropriate measures are taken to protect it against accidental or unlawful destruction, loss, alteration, damage, unauthorised disclosure or access.

In order to protect the electronically managed data files in the different registers, appropriate technical arrangements should be in place to ensure that data stored in the registers cannot be directly linked and attributed to the data subject.

Our computer systems and other data storage locations used in the provision of our services are located at our seat and at our data processors.

Both our IT systems and networks and those of our partners are protected against computer fraud, espionage, sabotage, vandalism, fire and flood, computer viruses, computer intrusions and denial of service attacks. Security is ensured through server-level and application-level protection procedures.

We use computer software that meets the requirements of data security for electronic data processing and record keeping. The program ensures that access to the data is limited to the persons who need it for the performance of their tasks, and only for the purpose for which it is intended and under controlled conditions.

We continuously ensure the appropriate physical protection of data and the devices and documents that carry them.

The IT tools we use to process personal data in the provision of our services are selected and operated in such a way that the data processed:

a) is accessible to authorised persons (availability);

b) its authenticity and authentication is ensured (authenticity of processing);

c) its integrity can be verified (data integrity);

d) is protected against unauthorised access (data confidentiality)

.

We take the following measures to reduce the risk of unauthorised access to the data provided by users when registering in the event of an unauthorised intrusion:

* Application of firewall, proper virus protection;
* Periodic log analyses based on the logs of IT systems;
* Regular IT maintenance, auditing, regular monitoring of IT systems;
* Access to the servers is restricted to the administrator and the Controller’s managing director and is possible only by using a private key, in addition to the username/password pair. It is not possible to log in without keys. The data is not accessible by any employee or fulfilment partner other than the Controller and the administrator, so there is no need to control internal access rights to the data;
* MultiAppsFactory Kft.’s computer equipment, systems, data storage facilities and devices are located at the seat of MultiAppsFactory Kft.
* Each computer is protected by a unique password.
* The data is stored in a database / mail server. The mail server can be accessed with an email / password pair. The database is not accessible to external applications.
* Some systems require the user to use two-factor authentication.
* Paper-based documentation is kept in a special and lockable cabinet, records are kept and regularly reviewed, and compliance with legal requirements is checked on an ongoing basis.
	+ - * Contributions, subscriptions, etc. are saved by the systems in an identifiable way. The Controller protects access to documents and its desktop computer with an appropriate password strength and other security measures.

Electronic messages transmitted over the Internet, regardless of protocol (email, web, ftp, etc.), are vulnerable to network threats that could lead to fraudulent activity, contract disputes, or the disclosure or modification of information. We take all reasonable precautions to guard against such threats. Systems are monitored to ensure that any security discrepancies are recorded and evidence is provided for any security incidents. System monitoring also makes it possible to check the effectiveness of the precautions taken.

Backups are available for 30 calendar days, with data broken down to days, stored on a disk on a separate device, from which all data can be restored if justified and necessary.

The existing security measures are sufficient to manage the risks, based on the current state of the art and our experience from our past activities.

**IV. RIGHTS AND OBLIGATIONS IN RELATION TO PERSONAL DATA BREACHES**

A personal data breach occurs when personal data or information is inadvertently or unlawfully:

- destroyed,

- lost,

- modified,

- disclosed without authorisation, or

- becomes accessible to unauthorised persons.

Depending on the extent to which the breach compromises the rights and freedoms of natural persons, the GDPR imposes a notification obligation on us as Controller.

If a personal data breach occurs, we will notify it to the competent supervisory authority without undue delay in accordance with our obligation under Article 33 of the GDPR. We may only waive this requirement if the personal data breach is unlikely to pose a risk to the rights and freedoms of natural persons.

If the personal data breach is related to the activities of the processor, the processor must notify us without undue delay. We do the same when we are in the role of processor.

When a personal data breach occurs, we shall take prompt action to remedy the data breach, taking into account the need to mitigate or prevent any adverse consequences that may result from the breach.

We keep records of personal data breaches.

The purpose of the register is to enable us to demonstrate compliance with the GDPR when being audited by the National Authority for Data Protection and Freedom of Information (NAIH) as supervisory authority.

The Controller should notify the personal data breach to the NAIH without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the Controller is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

We shall also inform data subjects immediately of a personal data breach if it poses a high risk to their rights and freedoms.

If a high-risk personal data breach involving the personal data of data subjects occurs during our processing, we shall inform data subjects of the following facts and circumstances:

- a description of the personal data breach,

- name and contact details of the contact person responsible for data protection matters,

- a description of the likely consequences of the personal data breach,

- a description of the measures planned or taken by the controller to remedy the breach, including measures to mitigate any adverse consequences of the personal data breach.

Details of how we handle data breaches are set out in our Personal Data Breach Management Policy.

**V. THE RIGHTS OF THE DATA SUBJECT**

Your rights are explained in more detail below. The following rights are not absolute: their exercise may be subject to conditions or exceptions.

We can comply with your request to enforce your rights if we are permitted to do so under data protection law or if we are required to do so under legal provisions on data protection. The provisions of this Privacy Policy do not and shall not give you any rights that go beyond the requirements of data protection legislation.

| **DATA SUBJECT’S RIGHT** | **CONTENT** |
| --- | --- |
| * 1. **Right to transparent information**
 | You have the right to be provided with clear, transparent and easy-to-understand information about how we process your personal data and what rights you have in relation to processing. We comply with this obligation in this Privacy Policy.  |
| * 1. **Right of access to personal data**
 | You have the right to be informed whether we process your personal data and, if we do, which personal data we process and how we process it. The purpose of this is to ensure that our data processing activities concerning you are transparent, so that you can check that we comply with data protection law. We may deny access to your personal information only if it could disclose personal information about another person or otherwise adversely affect the rights of another person. |
| * 1. **The right to rectification**
 | You may ask us to take reasonable steps to rectify your personal data if you believe that we are inaccurately processing your personal data. |
| * 1. **Right to erasure**
 | This right is also known as the “right to be forgotten” and allows you to ask us to delete or remove your personal data if there is no compelling reason for us to continue to process it or if its use is unlawful. The right to erasure is not a general right, there are exceptions, e.g. where the processing of your personal data is justified by defence of legal claims.  |
| * 1. **Right to restriction of processing**
 | You have the right to “block” or disable further use of your personal data until we have assessed your request for rectification or, as an alternative to deletion. If the processing is restricted, we may continue to store your personal data, but we may not further use it without your consent or without authorisation by law. To comply with this restriction, we keep a list of those who have “blocked” the use of their personal data.  |
| * 1. **Right to data portability**
 | You have the right to receive the personal data we process on a storage medium and to have it transferred to another controller, provided that the processing of your personal data is based on your consent or on a contract between us or is carried out by automated means.  |
| * 1. **Right to object**
 | You have the right to object to the processing of your personal data on grounds relating to your particular situation, provided that the processing is based on legitimate interests. In this case, we may continue to process your personal data only if we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.  |
| * 1. **Right to legal redress**
 | If your rights have been infringed, you can take your case to the National Authority for Data Protection and Freedom of Information or to court; you can find out how below. |

In the exercise of your rights as data subject, we shall inform you of the decisions taken in response to your request and of the measures planned or implemented without undue delay, but no later than thirty days after receipt of the request. The information shall be provided through the same channel you used when you made the request, unless you specifically request otherwise.

**VI. WHO TO CONTACT IF YOU HAVE A QUESTION OR WISH TO SEEK REDRESS?**

If you would like to receive more information about the processing of your personal data or wish to exercise any of the above rights, or if you are dissatisfied with the way we have processed your personal data, please contact us.

**If you have any questions or comments, you can contact the Controller directly:**

Email: info@multiappsfactory.hu

Please provide as much information as possible so that we can more easily identify the information you are requesting, the action you want to be taken and why you think this should be done.

We may ask for additional information to identify you before we process your request. If you do not provide the requested information and we are unable to identify you as a result, we may refuse to comply with your request.

You can submit requests related to our services in writing by email.

Similarly, a request received from an email address previously provided to us shall be considered as a request from the data subject.

In the case of complaints or claims submitted from other email addresses and in writing, the person submitting the complaint or claim must duly prove their data subject status. In the absence of proof of the data subject status, we are not in a position to assess or fulfil the claim.

We will normally reply to your request within one month of receiving it. This period may be extended by a further two months if necessary, taking into account the complexity and number of the requests you have made.

We do not charge a fee for such communications or our activities, except:

* if you request additional copies of the personal data we process, we may charge you our reasonable administration costs, or
* if you make manifestly unfounded or excessive requests, in particular because of their repetitive nature, in which case we may charge you reasonable administrative costs or refuse to comply with the request.

Complaints, questions and requests sent to us shall be stored for 6 months from the date of submission and then deleted, with the exception of correspondence relating to pending cases. If a legal claim arises in the case, the data shall be retained within the time limit for enforcing the claim, which is typically 5 years (see: Act V of 2013 on the Civil Code).

**Procedure of the Data Protection Authority**

National Authority for Data Protection and Freedom of Information

Registered seat: H-1055 Budapest, Falk Miksa utca 9-11,

Mailing address: H-1374 Budapest, Pf. 603.

Phone: +3613911400

Email: ugyfelszolgalat@naih.hu

Website: <http://www.naih.hu>

**Right to apply to the courts**

In the event of an alleged impairment of rights in relation to the processing of your personal data, you can also apply to the court with territorial jurisdiction (contact details here: https://birosag.hu/torvenyszekek), which is the Budapest-Capital Regional Court (H-1055 Budapest, Markó u. 27.) in the capital city. The action may also be brought before the court of the data subject’s domicile or place of residence, at the data subject’s choice.

**VII. AMENDMENT OF THE PRIVACY NOTICE**

As Controller, we reserve the right to unilaterally amend this Privacy Policy at any time.

After the modification, the user accepts the provisions of the Privacy Policy in force at the time of the next login, and no additional consent of the individual user is required.

09.04.2025

1. REGULATION (EU) 2016/679/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [↑](#footnote-ref-1)