**GENERAL PRIVACY POLICY**

**OF**

**MULTIAPPSFACTORY LTD.**

MultiAppsFactory Kft., which operates an online radio media content aggregator service on the website https://myonlineradio.at (hereinafter: Website) and in the iOS, Android and television applications of Myonlineradio.at (hereinafter: Application), as data controller (hereinafter: Data Controller, we) hereby informs the data subjects (visitors and users of the Website and the Application, the contacts of our business partners who are interested in our services and who use our services) that, while respecting the data subjects' personal rights and privacy, during data processing, the present general data management acts in accordance with the information provided (hereinafter: Privacy Policy).

1. **GENERAL INFORMATION REGARDING DATA PROCESSING**

**1. WHAT DOES DATA PROTECTION MEAN AND WHY IS IT IMPORTANT?**

Data protection is a set of principles, rules, procedures, data management tools and methods that ensure the lawful processing of personal data and the protection of data subjects, with the aim of protecting the rights of data subjects and preventing unauthorized access to personal data.

Data protection is an important means of protecting the privacy, which do not actually protect the data, but its owner.

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

In the course of its business activities, the Data Controller processes the personal data of the following data subjects (hereinafter: Data Subject, Data Subjects, You):

• 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: Online Radio).

In this Privacy Policy, and wherever your personal data is used, we provide concise, transparent and intelligible information about the method, purpose and circumstances of data management, using clear and plain language.

In all cases, the personal data made available to us will be handled in accordance with the applicable Hungarian and European Union data protection legislation and legal practice, and in all cases we will take the technical and organizational measures for ensuring the security of the processing. Respecting the basic principle of accountability, we continuously provide up-to-date and comprehensible information about our data processing activities.

In view of changes in legislation and the continuous development of jurisprudence, as well as changes in the services we offer, we reserve the right to continuously update the Privacy Policy.

You can always access the current version of the Privacy Policy, as well as the previously effective versions, under the menu item https://myonlineradio.at/public/docs/privacy-policy/de\_AT/.

1. **Definitions**

Knowledge of the basic concepts of data protection is essential for the interpretation of this Privacy Policy. The definitions are contained in Article 4 of the GDPR, from which we highlight the following:

**‘Personal data’** means any information relating to an identified or identifiable natural person ("data subject");

**‘An identifiable natural person’** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**’Data subject’** is any identified or identifiable natural person, whose personal data is processed by the controller responsible for the processing;

**’Special categories of personal data’** are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic and biometric data for the unique identification of natural persons, health data and the sexual life or sexual orientation of natural persons; personal data which are prohibited under Article 9 (1) of the GDPR may be processed only in the exceptional cases provided for in Article 9 (2) of the GDPR, in particular with the express consent of the data subject;

**’Processing’** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means

**’Data processing operations’** are 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’** is making the data available to anyone;

**‘Deletion of data’** is making data unrecognizable in such a way that their recovery is no longer possible;

**‘Filing system’** means 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’** means the marking of stored personal data with the aim of limiting their processing in the future;

**‘Profiling’** means 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’** means 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 or controller responsible for the processing’** is anyone who determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**’Processor’** is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

 **’Consent** of the data subject’ is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

 **’Recipient’** is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

**’Third party’** is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

‘**Personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

**‘Newsletter’** is an electronic mail, transactional, advertising or other campaign information sent to the e-mail address of persons subscribed to an address list, typically created automatically and sent by an application designed for this purpose;

**‘Facebook pixel (Facebook cookie)’** is a code with the help of which a report is prepared on the Website about conversions, target audiences can be compiled, and the owner of the page receives detailed analysis data about the visitors' use of the Website. With the help of the Facebook remarketing pixel tracking code, you can display personalized offers and advertisements on the Facebook interface to Website visitors. The Facebook remarketing list is not suitable for personal identification (fr, tr).

More information about the Facebook Pixel can be found here: https://www.facebook.com/business/help/651294705016616

**‘Adblock Plus’** blocks all annoying ads on the web by default, including video ads on YouTube, Facebook ads, flashy ads, pop-ups, pop-up screens, and more. This is possible based on the selected filter list(s). Simply install Adblock Plus and, if you like, customize it to suit your unique browsing needs.

**4. PURPOSE OF PRIVACY POLICY**

The purpose of this Privacy Policy is to provide easily transparent and understandable information for those concerned that

o how we collect your personal data on the Website and Application, for what purpose we use it, and according to what principles and rules we handle your personal data,

o what personal data is processed during the provision of the Priority Position and Premium Partner Services for Online Radios (hereinafter: ‘Services Provided to Online Radios’), as well as Basic Services and Premium Services provided to Users (hereinafter: ‘Services Provided to Users’) (‘Services Provided to Online Radios’ and ‘Services Provided to Users’ together: the ‘Services’),

o under what circumstances we may transfer your personal data to others and

o what rights you can assert in relation to the processing of your personal data.

**5. PERSONAL AND OBJECTIVE SCOPE OF THE GENERAL DATA MANAGEMENT INFORMATION**

The personal scope of this Privacy Policy extends to visitors interested in the Services provided by the Data Controller and available on the Website, as well as users and Online Radios using the Data Controller’s Service, contacts of the contractual partners of the Data Controller, and the Data Controller, as well as the Data Processors.

In this Privacy Policy, the Data Controller provides detailed information on the essential circumstances, methods, principles, legal basis, purpose and duration of data processing related to its Services.

**6. PRINCIPLES OF DATA PROCESSING**

| **ADATVÉDELMI ELV** | **TARTALMA** |
| --- | --- |
| * 1. **Lawfulness, fairness and transparency**
 | Data processing must be legal, fair and transparent during the entire period of data processing. |
| * 1. **Purpose limitation**
 | The principle of purpose limitation means that we can only process your personal data for a clearly defined, legitimate purpose, and that the collection of data and other data processing operations must be aligned with the purpose of data processing. It follows from the principle of purpose-boundness that personal data can only be processed until the purpose of data processing is achieved. |
| * 1. **Data minimisation**
 | The principle of data minimistion means that only those personal data that are absolutely necessary to achieve the data processing goals can be processed legally. |
| * 1. **Accuracy**
 | The principle of accuracy means that the data stored in our filing systems must correspond to reality in the entire process of data processing. If the data is inaccurate or incorrect, based on your request, we will work with you to restore the accuracy of your personal data. |
| * 1. **Storage limitation**
 | The principle of storage mimitation means that personal data can only be stored as long as the purpose of data management is achieved. Personal data cannot be accumulated or stored indefinitely. To this end, we determine the duration of data processing and, if this is not possible, the criteria for determining the duration. |
| * 1. **Integrity and confidentiality**
 | As a data controller, we treat the personal data transferred to us confidentially. Your personal data can only be accessed by our employees and agents who are entitled to data management based on their job or duties. We take care of the preservation of documents and data containing personal data with technical and organizational security measures in line with the state of the art and expected of similar organizations. |
| * 1. **Accountability**
 | The principle of accountability means that, as a data controller, we must be able to prove the legality of data protection, i.e. compliance with the provisions of the GDPR. For the sake of accountability, we document our data management activities in accordance with the provisions of the GDPR.We keep a record of the transfer and publication of the necessary information, the data management we carry out, the measures we take for the sake of data security, data protection incidents, and inquiries related to data protection. |

**7. WHAT PERSONAL DATA CAN WE PROCESS?**

Depending on how you use our Website and Application, and what information you share with us when interested in or using our Services, we may collect the following personal data from you:

a. name (surname and/or first name)

b. e-mail address

c. residential address or billing address (country, city, postal code, house number)

d. tax number (only in case of invoice request)

e. phone number (business or personal)

f. username

g. password entered during registration

h. any other personal information you share with us when filling out a contact form

i. the personal information and your opinion that you share with us during the completion of the test or survey and when recommending our service on the website

j. IP address, password, login data (e.g. registration date), cookies and other technical information from which we can find out how you use our website

k. position and name of the employer

l. your personal information provided during complaint handling.

**8. WHAT DO WE USE YOUR PERSONAL DATA FOR?**

a. You can inquire about our services by filling out the contact form.

b. In accordance with the principle of accountability, in order to ensure technical and security requirements, we automatically log the technical data and conversion events of the users of the Website, which are generated during the use of the Services, based on its legitimate interest.

c. We use the data of our business partners' contacts in connection with the creation, performance and termination of contracts, as well as for the purpose of recommending additional Services related to the Services used and for the purpose of fulfilling accounting obligations.

d. In order to create, fulfill, modify and terminate the contract, we process the data of the persons designated as contact persons.

e. Based on your complaint, your personal data is also required for your identification and contact in order to carry out the complaint procedure.

We use your personal data collected using cookies and social media pixels

in order to operate the Website, facilitate its use and security, as well as to monitor and analyze user activities on the Website, as well as to display relevant advertisements, we use cookies, most of which cannot be used for personal identification in the absence of additional information, but in some cases the cookie also contains a cookie identifier suitable for unique identification. You can read 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 advertisements and remarketing activities for the social media service provider. We cannot link this data to your person. We also provide information on the details of this in the Cookie Policy.

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

The personal data of the data subjects can be processed on the following legal bases according to the GDPR:

• the Data Subject has given his consent to the processing of his personal data for one or more specific purposes;

• data processing is necessary to fulfil a contract in which the Data Subject is one of the parties, or it is necessary to take steps at the Data Subject's request prior to the conclusion of the contract;

• data management is necessary to fulfil the legal obligation of the Data Controller;

• the data processing is necessary to enforce the legitimate interests of the Data Controller or a third party, and the Data Controller has determined through an interest assessment test that the interests or fundamental rights and freedoms of the Data Subject that require the protection of personal data do not take priority over these interests.

**II. DETAILED INFORMATION REGARDING CERTAIN DATA PROCESSINGS**

**1. DATA PROCESSES AFFECTING USERS**

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

**Data Subjects:** Website users who wish to contact Myonlineradio by filling out the contact form

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

**Source of data:** in terms of name and e-mail address, directly the data subject, in terms of personal data that may appear in the subject and text of the message, the user, who is obliged to ensure the consent of the data subject

**Purpose of data processing:** identification, contact, providing answers to the user's interests and questions, providing assistance related to the use of services

**Legal basis for data processing:** freely given consent of the data subject based on point a) of Article 6 (1) of the GDPR

**Duration of data processing:** until the withdrawal of the data subject, but for a maximum 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

**Does data transfer take place:** no, with the exception of data processors providing IT services and hosting services

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

**Data Subjects:** Website users who wish to contact Online Radio by filling out the contact form

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

**Source of data:** in terms of name and e-mail address, directly the data subject, in terms of personal data that may appear in the subject and text of the message, the user, who is obliged to ensure the consent of the data subject.

**Purpose of data processing:** based on the agreement concluded with Online Radio, Myonlineradio makes it possible to contact the Online Radios available in the Hyperlink library of the Website via the contact form on the Website, using the e-mail address available on the Online Radios' own website. With regard to the personal data provided in the contact form, Myonlineradio and Online Radio are considered separate data controllers, as the personal data are handled for different purposes. The sole purpose of Myonlineradio's data processing is to be able to exclude potentially spamming and harassing users from using the site, and to report the error to the user in the event of an email sending error.

**Legal basis for data processing:** freely given consent of the data subject based on point a) of Article 6 (1) of the GDPR

**Duration of data processing:** until the withdrawal of the data subject, but for a maximum of six months.

**Possible consequences of failure to provide data:** in the absence of data, the Data Controller cannot filter out spamming users and cannot check that a user cannot send more than three contact forms a day

**Does data transfer take place:** no, with the exception of data processors providing IT services and hosting services

* 1. **PHOTOS AND VIEOS SHOWN ON THE MYONLINERADIO FACEBOOK PAGE**

**Data Subjects:** Data Subjects appearing in photos related to news about public figures used on Myonlineradio's Facebook page, as well as in funny pictures

**Personal data processed:** name, image, video recording, sound

**Data source:** third party

**Purpose of data processing:** to inform and entertain the followers and visitors of the Myonlineradio Facebook page

**Legal basis for data processing:** data processing related to journalism, the Data Controller has a legitimate interest in informing and entertaining users when editing the content of the Facebook page based on GDPR Article 6 (1) point f)

**Duration of data** **processing:** until the content is deleted from our Facebook page

**Possible consequences of failure to provide data:** in the absence of data provision, the Data Controller cannot publish informative and entertaining content containing images of the data subjects to users on its Facebook page.

**Will data be transferred:** no, with the exception of Meta Platforms Ireland Ltd, which operates the Facebook service

* 1. **POSTING COMMENTS USING THE WEBSITE EMBEDDED FACEBOOK COMMENT PLUGIN**

**Data Subjects:** users who can comment on the content of the Website via their Facebook account, and can also share their comments with their Facebook friends

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

**Source of data:** the data subject via an external service provider

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

**Legal basis for data** **processing:** publication can take place after the data subject has logged in to Facebook and given the data subject's consent based on Facebook's data privacy policy enabling this embedding

**Duration of data** **processing:** until the data subject's registration is removed by himself or until the given content is deleted from our website

**Will data be transferred:** no, with the exception of Meta Platforms Ireland Ltd, which operates the Facebook service

* 1. **DATA PROCESSING RELATED TO ONLINE RADIO AUDIENCE MEASUREMENT**

**Data Subjects:** subscribers to the Premium Service of Myonlineradio

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

**Source of data:** the Data Subject

**Purpose of data processing:** the legitimate interest of the Data Controller to be able to account for the revenue share based on the listening data based on the contract concluded with Online Rádio for the Premium Partner Service

**Legal basis for data** **processing:** the Data Controller's legitimate interest in Article 6 (1) of the GDPR according to point f).

**Duration of data** **processing:** based on the service contract with Online Radio for the given year, until the payment obligation is fulfilled

**Will data be transmitted:** Online Radio can view the measurement of listening at the request

**f. DATA PROCESSING RELATED TO THE EMBEDDING OF ONLINE RADIO ON THE WEBSITE**

**Data Subjects:** users of the Website

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

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

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

**Legal basis for data** **processing:** in the case of audience measurement cookies, the legitimate interest of the Data Controller According to point f) Article 6 (1) of the GDPR; in the case of other cookies, the freely given consent of Data Subject specified in point a) Article 6 (1) of the GDPR

**Duration of data** **processing:** according to the Cookie Management Platform and Cookie Policy, it varies for each cookie

**Will data be transferred:** in the case of third-party cookies, the personal data stored in the cookies will be transferred to the external service provider that placed the cookie on the Website

1. **WEBSERVER 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 the visit, address of the page visited and time spent there, IP address of the user's computer, type and version of the operating system and browser, as well as user searches

**Source of data:** the Data Subject

**Purpose of data processing:** during visits to the Website, the Data Controller records visitor data in order to check the operation of the Services and the Website functions and to prevent abuse.

**Legal basis for data** **processing:** the Data Controller has a legitimate interest in identifying users and preventing abuses [GDPR Article 6 (1) para. point f)]

**Duration of data** **processing:** one month

**Possible consequences of failure to provide data:** control of the functioning of the Services and the functions of the Website, prevention of abuse is not possible in the absence of managed visitor data. The Data Subject cannot object to the data recording, because the data processing is justified by compelling legitimate reasons (currently widely used technical solutions), without which the provision of the given Service is not possible.

**Does data transfer take place:** no, with the exception of data processors providing IT services and hosting services

**3. DATA OF ONLINE RADIOS AND BUSINESS PARTNERS**

**Data Subjects:** private users of the Data Controller's Services

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

**Data source**: the Data Subject

**Purpose of data processing:** using the Data Controller's services, maintaining contact, registering partners, distinguishing them from each other, using the Service, fulfilling payment obligations, invoicing

**Legal basis for data** **processing:** data processing is necessary for the fulfilment of the contract [GDPR Article 6 (1) para. point b)], in the case of invoicing data, GDPR Article 6 (1) point c), the (data processing is necessary to fulfil the legal obligation of the Data Controller, with regard to Section 169 (2) of the Accounting Act).

**Duration of data** **processing:** in the case of a contract, 5 years after the termination of the contract, with regard to invoicing data, In accordance with § 169, paragraph (2) of Accounting Act, 8 years, in the absence of a contract, up to 6 months from the date of contact

**Possible consequences of failure to provide data:** conclusion of a contract, fulfilment of payment obligations and invoicing are not possible in the absence of processed personal data.

**Does data transfer take place**: no, with the exception of data processors providing IT services and hosting services

**4. CONTRACTS OF ONLINE RADIO AND COMPANIES CONTRACTING WITH THE DATA CONTROLLER**

**Data Subjects:** employees of third parties (Online Radios, other businesses) designated as contact persons in the performance of the contract, who contract with the data controller, or persons in a legal relationship with them for other work purposes

**Personal data processed:** surname, first name, e-mail address, phone number, position, other data on the business card

**Source of data:** contractual partner of the Data Controller

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

**Legal basis for data** **processing:** in order to conclude, fulfil and terminate the contract, the legitimate interest in facilitating the cooperation of the parties and implementing communication between the parties based on Article 6 (1) point b) of the GDPR.

(An interest assessment test is available upon request.)

**Duration of data** **processing:** until the business relationship with the given contractual partner is terminated or there is no change in the contact person at the given contractual partner.

**Does data transfer take place:** no, with the exception of data processors providing IT services and hosting services

**5. DATA PROCESSING RELATING TO PERSONS COOPERATING IN OTHER LEGAL RELATIONS RELATING TO THE PERFORMENCE OF WORK**

**Data Subjects:** natural persons who have a contract or business relationship with the Data Controller

**Personal data processed:** name, address, e-mail address, mother's name, place of birth, time, tax identification number, tax number, contact information, personal identification document, passport number, bank account number of natural person contributors (suppliers) contracting with the Data Controller

**Source of data:** the Data Subject

**Purpose of data processing:** the conclusion, fulfilment, termination of the contract between the Data Controller and the data subject, the fulfilment of the statutory preservation obligation for tax documents and accounting documents, the provability of the content of the contractual relationship in the event of a claim or legal dispute

**Legal basis for data** **processing:** The legal basis for data management in the context of the registration of the contracting party's data is the performance of the contract based on Article 6 (1) point b) of the GDPR.

With regard to the issuance and preservation of accounting documents, the legal basis for data management is the fulfilment of the legal obligation of the Data Controller based on Article 6 (1) point (c) of the GDPR.

**Duration of data** **processing:** Based on the Data Controller's obligation according to § 169 of Act C of 2000 on accounting (hereinafter: "Accounting Act"), the accounting documents for 8 (eight) years after the termination of the Contract, in the event of a legal dispute, if the at a later date, fulfilling its legal obligation for 5 (five) years after the conclusion of the legal dispute

**Does data transfer take place:** no, with the exception of data processors

**6. COMPLAINT HANDLING**

**Data Subjects:** users who submit complaints about the Service

**Personal data processed:** surname, first name, e-mail address, telephone number, billing name, address, tax number

**Source of data:** the Data Subject

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

**Legal basis for data** **processing:** on the basis of Article 6 (1) point c) of the GDPR, fulfilling the obligations of the data controller according to paragraph (7) 17/A of Act CLV of 1997 on consumer protection according to which the company must keep the record of the complaint and a copy of the response for three years, and present it to the inspection authorities at their request

**Duration of data** **processing:** Copies of the protocol, transcript and the response to the objection must be kept for 3 years as set out in 17/A. § (7) of Act CLV of 1997 on consumer protection.

**Does data transfer take place:** no, with the exception of data processors

**10. PROVISIONS REGARDING DATA MANAGEMENT OF MINORS**

The legal representative can give consent to data processing on behalf of minors who have not reached the age of 14 and those otherwise incapacitated.

A minor who has reached the age of 14, as well as a data subject with otherwise limited legal capacity, may consent to data processing with the consent or subsequent approval of their legal representative.

The Data Controller offers its Service to persons over 18 years of age, however, it is not in a position to check the consent of the consenting person or to know the contents of the declaration of the legal representative, so the person concerned or his legal representative guarantees that the consent complies with the law. When using the Service, the Data Controller considers the appropriate consent of the legal representative to be given.

**11. WHO WILL BE AUTHORIZED TO HANDLE YOUR PERSONAL DATA?**

We, as the Data Controller, determine the purpose and means of processing your personal data.

**DATA CONTROLLER DATA:**

Company name: MultiAppsFactory Limited Liability Company

Headquarters: 1024 Budapest, Margit krt. 57. 2nd em. 5.

Tax number: 26278823-2-41

Company registration number: 01-09-357239

Managing Director: Attila Szabó

E-mail address: info@multiappsfactory.hu

Telephone: +36-30/813-2598

As a data controller, we treat the personal data provided to us confidentially. Your personal data can only be accessed by our employees and agents who are entitled to data management based on their job or duties.

**12. WHO CAN WE SHARE YOUR PERSONAL DATA WITH?**

**DATA PROCESSORS**

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

The data processors will handle your personal data on our behalf, strictly according to our instructions and providing appropriate guarantees.

We share your personal data, we may also share:

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

**JOINT DATA CONTROLLING**

With regard to embedded content, external service providers (Meta Platforms Ireland Ltd, Online Radios) collect and transmit personal data through pixels, Myonlineradio and the social media provider are joint data controllers.

You can read more about the pixels used on the website in the Cookie Policy.

**EXTERNAL SERVICE PROVIDERS**

In connection with the provision of the Services, the Data Controller uses external service providers in many cases, which cooperates with external service providers.

Regarding the personal data processed in the systems of external service providers, the guidelines are contained in the privacy policy of the external service providers. The Data Controller will do everything in its power to ensure that the external service provider processes the personal data transmitted to it in accordance with the law and uses them exclusively for the purposes specified by the data subject or set out in this Privacy Policy.

The Data Controller informs the Users about the transfer of data to external service providers in the framework of this Privacy Policy.

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

Your data in the contact form will be processed at most until you withdraw your consent (but a maximum of 6 months).

If you use our Services, or if a contract is concluded between us, your personal data processed on the basis of the contract concluded between us under the legal title of fulfilment of the contractual obligation, after the termination of the contract, according to the statute of limitations of the Civil Code, we process it until 5 years have passed.

In case of use of the Service or a contractual relationship, your invoicing data will be processed by the Data Processor commissioned by us for a maximum of 8 years based on legal authorization, after which this data will be deleted.

In the case of a post containing personal data published on our Facebook page, we process the data until the content is deleted from our Facebook page, and in the case of comments published with the help of Facebook modules embedded in our page, until the post of the person concerned is removed by himself, or until the given content is deleted from our website.

In the case of data processing related to complaint handling, copies of the minutes, transcripts and the response to the complaint must be kept for 3 years as set out 17/A. § (7) in the Act CLV of 1997 on consumer protection.

**14. DATA PROCESSORS**

Some personal data provided to us may be forwarded to the data processors engaged by us, in view of the purpose of the data processing. The data processors process the received personal data in accordance with the provisions of the data processing contract concluded with the data controllers and may not use them for other data management purposes.

Our permanently cooperating data processors are the following:

|  |  |  |
| --- | --- | --- |
| **DATA PROCESSING ACTIVITY** | **NAME** | **ADDRESS, CONTACT** |
| **IT operation and system administrator services** |  | Address: Website: E-mail:  |
| **Hosting service** | Rackforest Informatikai Kereskedelmi és Szolgáltató Kft. | Address: 1132 Budapest, Victor Hugo utca 18-22. 3. em. 3008.Website: www. rackforest.com E-mail: info@rackforest.hu |
| **Accounting and payroll services** | Forgóeszköz Kft. | Address: 1083 Solymár, Orgona utca 7.E-mail:  |
| **Invoicing, automatic invoice issuance** |  Billingo Technologies Zrt. / billingo.hu | Address: 1133 Budapest, Árbóc utca 6. I. meletWebsite: https//www.billingo.huEmail: hello@billingo.hu |

**GENERAL CONTRACTUAL TERMS OF DATA PROCESSING BY DATA PROCESSOR**

**In accordance with the GDPR, the data processor undertakes to:**

|  |  |
| --- | --- |
| (a) | processes 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, unless that law prohibits such information on important grounds of public interest; |

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| (c) | takes all measures required pursuant to Article 32 of GDPR;

|  |  |
| --- | --- |
| (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 and access to personal data in a timely manner in the event of a physical or technical incident; |

|  |  |
| --- | --- |
| (iv) | a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. |

 |

|  |  |
| --- | --- |
| (d) | respects the conditions for engaging another processor; |

|  |  |
| --- | --- |
| (e) | taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in GDPR |

|  |  |
| --- | --- |
| (f) | assists the controller in ensuring compliance with the obligations pursuant to the provisions on Security of personal data taking into account the nature of processing and the information available to the processor; |

|  |  |
| --- | --- |
| (g) | at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; |

|  |  |
| --- | --- |
| (h) | makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. |

1249 / 5000

(i) upon termination of the provision of the data processing service, at the discretion of the Data Controller, delete or return all personal data to the Data Controller and delete existing copies, unless Union or Member State law provides for the storage of personal data;

(j) provide the Data Controller with all information necessary to verify the erasure of the data or copies and to enable and facilitate audits, including on-site inspections, by the Controller or another auditor appointed by him. The Data Processor shall immediately inform the Data Controller if it considers that any of its instructions violate this GDPR or the data protection provisions of the Member States or the Union.

k) report the data protection incident to the Data Controller within 72 hours of becoming aware of it. That notification shall include at least:

(i) a description of the nature of the data protection incident, including, where possible, the categories and approximate number of data subjects and the categories and approximate number of data affected by the incident; (ii) the name and contact details of the data protection officer or other contact person for further information;

j) provides the Data Controller with all information necessary to verify the deletion of data and copies, and which enables and facilitates audits conducted by the Data Controller or other inspectors commissioned by the Data Controller, including on-site inspections. The Data Processor shall immediately inform the Data Controller if it believes that any of its instructions violates this GDPR or national or EU data protection provisions.

k) reports the data protection incident to the Data Controller within 72 hours of becoming aware of it. In said notification, at least:

(i) the nature of the data protection incident must be described, including – if possible – the categories and approximate number of Data Subjects, as well as the categories and approximate number of data affected by the incident;

(ii) the name and contact details of the data protection officer or other contact person providing additional information must be provided;

(iii) the likely consequences of the data protection incident must be described; as well as

(iv) the measures taken or planned by the Data Processor to remedy the data protection incident must be described, including, where appropriate, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

l) supports the Data Controller in fulfilling the Data Subjects' requests to exercise one or more of their rights provided for in the GDPR;

m) if the Data Processor receives a request from any Data Subject to exercise one or more of the rights provided for in the GDPR, the Data Processor informs the Data Subject to contact the Data Controller directly with the request, and at the same time informs the Data Controller of the request without delay;

n) keeps all the records required in Article 30 (2) of the GDPR and, if the processing of personal data on behalf of the Data Controller makes this possible, makes these records available to the Data Controller upon request.

The Data Processor undertakes to handle the personal data it processes exclusively in accordance with the relevant legislation.

The Data Controller is entitled to check the performance of the activity specified in this contract, and in particular the method of storing and processing the personal data of the Data Subjects, once a year at a previously agreed time.

If the Data Processor suffers damage in connection with the Data Controller's activities, the Data Controller is obliged to compensate it. If the Data Processor initiates a claim for compensation or initiates proceedings in connection with the Data Controller's activities, the Data Controller is obliged to exempt the Data Processor from compensation, imposed fines, and penalties within 30 days.

**15. EXTERNAL SERVICE PROVIDERS**

A. Service providers operating webstores of applications

Service providers (e.g. Apple Inc., Google Inc.) operating mobile application stores (e.g. Apple Store, Android Store) process the data of the users of the services installed on the end-user device independently of us and send update notifications.

**B. Third party intermediary service providers**

1. When using the Services, some service providers (e.g. Google Inc., Twitter Inc., Facebook Inc., Pinterest Inc and Pinterest Europe Ltd., LinkedIn Corp.) provide applications that facilitate registration and access in accordance with their own data protection guidelines.

With regard to content made available within the framework of the Services and shared on various social media sites, the service provider enabling the sharing of the content is considered the controller of personal data, and its activities are governed by its own terms of use and data protection policy. Such external intermediary services

|  |  |  |
| --- | --- | --- |
| **EXTERNAL SERVICE PROVIDER** | **PRIVACY POLICY LINK** | **TERMS OF SERVICE LINK** |
| **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/hu/+/policy/](https://www.google.com/intl/hu/%2B/policy/) | [https://www.google.com/intl/hu/+/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> |

**2. Social media platforms**

Data processing within social media platforms (e.g. Facebook page) is always subject to the respective social media's own privacy policy, rules and practices, which are continuously published on the interfaces operated by the respective service provider. The social media platform and the Data Controller are joint data controllers.

There are share buttons on our Website that you can click to share content from our Website on social media channels such as Facebook. We do not use these buttons to share your personal data with social media providers. When you click on a share button, the relevant social media provider collects personal data directly from you. Please read the privacy policy of the social media providers you wish to share content with before clicking the appropriate share button.

The use of the "Like" and "Comment" social plugins requires that the user is logged in to their Facebook account and has consented to the placement of "Application and website cookies". If both requirements are met, the user will be able to 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. Third party web analytics and ad serving companies**

For the operation of our web-based services, we use the services of external web analytics and ad serving companies.

The web analytics and ad serving providers use measuring pixels in addition to cookies for the purpose of collecting information related to the measurement of user habits and the serving of advertisements, and the so-called campaign codes are used.

**Google Analytics**

On our website, we use the Google Analytics audience measurement service of Google Ireland Limited (Gordon House, Barrow Street, Dublin 4, Ireland), which uses cookies to analyze user behavior. Google Analytics also records the IP address of website visitors, but shortens it before storing or analyzing it, thereby anonymizing it (if technically possible). Anonymization takes place within the territory of 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.

When transferring data to a country outside the EEA, Google relies on the following compliance decisions in certain cases:

• conformity decisions of the European Commission;

• UK compliance decisions;

• Swiss compliance decisions.

Google does not combine the IP address transmitted by your browser with other data in connection with the Google Analytics service. When you visit our Website, Google may connect data about activities on our Website with data about activities on other websites that use our advertising services.

Google Analytics collects data in accordance with the measurement code configuration you have provided and Google advertising cookies.

In addition to the reports generated from website usage statistics, Google Analytics - together 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 Internet.

‘Google Signals’ is a new data collection function of Google Analytics introduced to increase the efficiency of remarking and reporting, which is suitable for tracking users who have activated the "Personalize ads" setting in their personal account with Google. Google Analytics tracks the sessions and device types of all users who sign in to their Google Account and convert. After activating the feature, Google Analytics can recognize 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 regarding the display of personalized ads, related data management, and deactivation of the function at the following address: <https://support.google.com/ads/answer/2662856?hl=hu>

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

When you visit our Website, your web browser automatically sends certain information to Google. This includes our website URL and your IP address. In addition, Google can set cookies in your browser or read 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 advertisements, protect against fraud and abuse, and personalize the content and advertisements displayed on Google and our partners' websites.

We also use conversion tracking cookies on our website so that Google Ads can provide us with conversion statistics about the effectiveness of our ads. This is how we obtain information about how many people clicked on our ad and from there on our website with the conversion tracking tag. In the process, we do not get access to any information that could be used to 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 customize the ads displayed in Google products, such as Google Search. For example, it uses such cookies to remember your most recent searches, your previous interactions with ads or search results from certain advertisers, and your visits to advertisers' websites. Ads conversion tracking uses cookies. To track sales and other conversions resulting from the ad, cookies are saved on the user's computer when that person clicks on an ad. Some of the common uses of cookies are: to select ads based on what is relevant to the user, to improve reporting on campaign performance, and to avoid showing ads that the user has already seen.

Google AdSense is an online advertising mediation service operated by Google Inc., whose primary purpose is the sale of Internet advertising surfaces. The essence of the service is that website owners can allow text, image and video ads to be displayed on their website after registration.

In the context of Google AdSense and Google Ads remarketing, Google Inc. places visitor-tracking cookies on users' devices, which monitor visitors' online behaviour and on the basis of which Google Inc. provides advertising based on user behaviour and interests makes it available to them on the Website. The tracking cookie enables Google Inc. to identify the website visitor on other websites as well.

The "Privacy Guidelines" of Google Inc. are available at <http://www.google.hu/intl/hu/policies/privacy/>

On the website of Google Inc., you can find additional useful information about Google Inc.'s activities related to data and about disabling cookies and personalizing ads: https://adssettings.google.com/anonymous

Also, other information is available on the following Google pages:

Google Adsense [https://policies.google.com/privacy](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 want to participate in conversion tracking, you can reject this by disabling the installation of cookies in your browser. After that, you will not be included in our conversion tracking statistics.

**Social media pixels**

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

With the help of the Facebook pixel, we can also analyze the effectiveness of our ads on Facebook for statistical and market research purposes. In doing so, we can find out whether users reached our website by clicking on the Facebook ad.

By embedding the Facebook pixel on 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 registers your visit to our website in your profile. The data obtained about you is anonymous to us, which means that we cannot find out your identity based on this. At the same time, your data is stored and managed by Facebook, so they can be linked to the given user profile.

When using Facebook pixels, the Data Controller (we) and Facebook are considered joint data controllers.

Facebook data processing is governed by its own privacy policy, so you can find more information about the operation of the remarketing pixel and the display of Facebook ads in general in Facebook's privacy policy at the following address: <https://www.facebook.com/policy.php>

On the following interface of Facebook, you have the option to prohibit the recording of data 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, meaning they apply to both desktop and mobile devices.

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

We provide detailed information on the use of cookies and social media pixels in the Cookie Notice, which can be accessed by clicking here.

**Monitoring the Online Radios’ audience**

In connection with the embedding of Online Radio, Myonlineradio does not directly collect personal data, but it monitors the popularity of the embedded Online Radio Media Content with the help of the Google Analytics cookie.

The terms of the contract with Online Radios are aligned with the popularity (audience) of the Online Radio, therefore the Data Controller has a legitimate interest in accordance with Article 6(1)(f) of the GDPR to obtain information about whether users, e.g. on what device and for how long they listen to the given Online Radio.

The purpose of the data management is for the Online Radios to receive statistical feedback about the radio habits of the users, about the Online Radio Media Content programs they like, in an anonymized way.

The measurement is done in such a way that, on one side, the user embeds Online Radio on the Website, but this is not yet the URL of the final audio stream. However, this URL already contains the URL of the page that performs the measurement, www.radiostat.info. On the www.radiostat.info page there is a control script that monitors whether users have a session cookie. If there is none, the server automatically sets a session cookie, which detects that if someone loads the Online Radio again, they should be counted as the same person from the point of view of the measurement. From here, the user is forwarded using the session check to the real listening URL, where the user's IP address, the generated session\_id, and the page from which it was opened are entered. This data is inserted into the URL, where there is a token identifier, using reverse coding. The server sends the token ID to www.radiostat.info in the background. Here, however, the side performing the measurement is no longer connected to the user, but to the server in the background.

On the other side, a specific radio server that, when connected, sends what URL stream has been loaded, so they get a decryptable data that is sent to Google Analytics every 5 minutes, indicating that the user is still listening to Online Radio.

If the user finishes playing, the radio server sends a request to www.radiostat.info again indicating that the user has finished listening to Online Radio. The system then automatically deletes the stored file.

In order to account for the income from the provision of the Premium Service, the Service Provider records which Online Radio program the User listened to, broken down into one-minute units. The User's data will not be forwarded to Online Radio, Online Radio can only access anonymized data. The purpose of the audience measurement is for the Service Provider to prepare a statement for the Online Radios by counting the one-minute units associated with listening to the given Online Radio, as to how many Users with subscriptions listened to the given Online Radio for at least one minute.

**Legal basis for data processing:** GDPR Article 6 (1) point f) - data proessing is necessary to enforce the legitimate interests of the data controller or a third party, unless these interests are overridden by the interests or fundamental rights and freedoms of the data subject, which are personal data their protection is necessary, especially if the child concerned is a child.

**Personal data processed:** IP address, the generated session\_id, the start of the login, the page from which the user logged in

**The retention period of the data generated in this way:**

When the session ends, the data is deleted.

**Data transfer:** the data stored in the token is sent to Google Analytics for analysis. After the analysis, the given radio only receives statistical data.

**III.DATA SECURITY**

The Data Controller reduces the risk that the data provided by users during registration may become available in the event of an unauthorized intrusion by:

The Data Controller and the Data Processor shall take appropriate technical and organizational measures to take into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of data processing and the varying likelihood and severity of risks to the rights and freedoms of natural persons. to guarantee a level of data security commensurate with the level of risk. The Data Controller complies with the principles of the GDPR. Contributions, subscriptions, etc. the systems are saved in an identifiable manner. Data controller protects access to documents and your desktop computer with a strong password - other security measures: firewall application, regular IT maintenance, control, closed system vpn access - documents are stored electronically, paper-based documentation is kept in an exceptional and lockable cabinet, records are kept , regular review, verification of compliance with legal requirements, the performance assistant employed outside the Data Controller does not have access to the data, so there is no need to control the internal access rights to the data.

Existing security measures are sufficient to manage the risks, based on the current state of technology and the experience gained from the Data Controller's activities to date.

1. **RIGHTS AND OBLIGATIONS RELATING TO PERSONAL DATA BREACH**

A PERSONAL DATA BREACH is when personal data or data are accidentally or unlawfully:

- destroyed,

- lost,

- altered,

- communicated unauthorized, or

- made unauthorized.

The GDPR imposes a notification obligation on the Data Controller, depending on the extent to which the incident endangers the rights and freedoms of natural persons.

Pursuant to Article 33 of the GDPR, the Data Controller is obliged to notify the incident to the competent supervisory authority without undue delay and may waive this incident only if the personal data breach is not likely to endanger the rights and freedoms of natural persons.

If the personal data breach occurs in connection with the activities of the data processor, it is obliged to notify it to the Data Controller without undue delay.

Upon the occurrence of a personal data breach, the Data Controller shall immediately take measures to remedy the personal data breach, taking into account the mitigation or prevention of any adverse consequences arising from the incident.

The Data Controller keeps a record of personal data breaches.

The purpose of the register is to enable the Data Controller to verify compliance with the GDPR during the audit of NAIH as the comptenet supervisory authority.

The Data Controller shall report the data breach to the NAIH without undue delay and, if possible, no later than 72 hours after the data breach became known to the NAIH, unless the data breach is likely to pose no risk to the rights and freedoms of natural persons.

The Data Controller is obliged to inform the data subject without undue delay about the personal data breach if it poses a high risk to the rights and freedoms of natural persons. If a high-risk personal data breach affecting the personal data of the data subject occurs during the data processing of the Data Controller, the Data Controller will inform the data subject of the following facts and circumstances:

 description of the personal data breach,

- the 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 incident, including measures to mitigate any adverse consequences of the personal data breach.

1. **RIGHTS OF THE DATA SUBJECT**

The data subject may contact the Data Controller regarding the enforcement of his / her rights related to data management and his / her questions at the contact details included in this Privacy Policy.

The Data Controller shall inform the data subject of his / her actions or the reasons for their non-compliance within one month after the submission of the data subject's request (the data subject may file a complaint in this connection), this period may be extended by 2 months if necessary.

The procedure is free of charge (if justified and not excessive) and preferably electronic.

The Data Controller shall inform all recipients to whom or with whom the personal data have been communicated of any rectification, erasure or restriction of data processing, unless this proves impossible or requires a disproportionate effort. Upon request, the Data Controller shall inform the data subject of these recipients.

| **ÉRINTETTI JOG** | **TARTALMA** |
| --- | --- |
| * 1. **Right to transparent information**
 | You have the right to receive clear, transparent and easy-to-understand information about how we process your personal data and what rights you can assert in relation to data processing. We fulfil this obligation in this privacy Policy. |
| * 1. **Right of access by the data subject**
 | You have the right to receive information about whether we process your personal data and - if we do so - which of your personal data and how we process them. The purpose of this is to make our data processing activities concerning you transparent for you, so that you can check whether we comply with the data protection legal regulations. We may deny access to your personal information only if it could reveal personal information about another person or would otherwise negatively affect another person's rights. |
| * 1. **Right to rectification**
 | You can ask us to take reasonable measures to correct your personal data if, in your opinion, we handle your personal data inaccurately. |
| * 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 processing it or if its use is unlawful. The right to deletion is not general, there are exceptions, e.g. if protection against legal claims justifies the processing of your personal data. |
| * 1. **Right to restriction of processing**
 | You have the right to "block" or disable the further use of your personal data until we have decided your request for correction or as an alternative to deletion. If processing is limited, we may still store your personal data, but we may not use it further without your consent or authorization by law. In order to comply with the 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 processed by us on a data carrier and forward them to another data controller - provided that the processing of your personal data is based on your consent or the contract between us, or the data processing is done in an automated manner. |
| * 1. **Right to object**
 | You have the right to object to the processing of your personal data on grounds related to your particular situation, if the data processing is based on a legitimate interest. In this case, we can only continue processing your personal data if we can prove that the data processing is justified by compelling legitimate grounds that take precedence over your interests, rights and freedoms, or that are related to the establishment, exercise or defense of legal claims. |
| * 1. **Right to a remedy**
 | In the event of a violation of your rights, you can contact the Hungarian National Data Protection and Freedom of Information Authority (NAIH) or a court, the method of which will be explained below. |

During the exercise of the data subject's rights, we will inform you about the decisions made following your request and the planned or implemented measures without undue delay, but no later than thirty days from the receipt of the request. We provide the information through the same channel that you used when submitting the request, unless you specifically request otherwise.

**VI. WHERE CAN YOU GO IF YOU HAVE A QUESTION OR WANT TO GET A LEGAL REMEDY?**

If you would like to request additional information regarding the processing of your personal data or wish to exercise any of the above rights of the data subject, and if you are not satisfied with the way we have processed your personal data, please contact us!

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

E-mail: info@myonlineradio.at

Phone: +36-30/362-2898

Please provide as much information as possible to help us identify the information you are requesting, the action you want to take, and why you think it should be done.

Before evaluating your request, we may ask for additional information in order to identify you. If you do not provide the requested information and as a result we are unable to identify you, we may refuse to fulfil your request.

You can submit requests related to our services in writing by e-mail.

In the same way, we consider a request received from the e-mail address previously provided to us as a request received from the data subject.

In the case of claims submitted from other e-mail addresses and in writing, the person submitting the complaint or claim must prove his/her involvement accordingly. In the absence of proof of involvement, we are unable to assess or fulfil the request.

We usually respond to your request within one month of its receipt. We may extend this period by another two months if necessary, taking into account the complexity and number of requests you submit.

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

- if you request additional copies of the processed personal data, we may charge our reasonable administrative costs, or

- if you submit manifestly unfounded or excessive requests, especially due to their repetitive nature, in which case we may charge our reasonable administrative costs or refuse to fulfil the request.

Complaints, questions and requests sent to us are stored for 6 months from the date of submission and then deleted, with the exception of correspondence arising from cases that are still in progress. If a legal claim arises in the case, the data will be preserved within the time limit for its enforcement - typically 5 years (see: Act V of 2013 on the Civil Code).

**Data protection authority procedure**

Hungarian National Data Protection and Freedom of Information Authority

(Nemzeti Adatvédelmi és Információszabadság Hatóság)

Headquarters: 1055 Budapest, Falk Miksa utca 9-11,

Mailing address: 1374 Budapest, Pf. 603.

Phone: +3613911400

E-mail: ugyfelszolgalat@naih.hu

Website: http://www.naih.hu

**Right to go to court**

In the event of a perceived violation of rights related to the handling of your personal data, you can also contact the competent court (contact details here: https://birosag.hu/torvenyszekek) or the Capital Court in the capital (1055 Budapest, Markó u. 27). At the choice of the data subject, the lawsuit can also be initiated before the court of the data subject's place of residence or residence.

Proceedings against the controller must be brought before the courts of the Member State in which the controller is established (Hungary),but may also be brought before the courts of the Member State of the habitual residence of the data subject.

**VII. AMENDING THE PRIVACY POLICY**

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

After the amendment, the user accepts the provisions of the Privacy Policy in force at all times with the next login, in addition, there is no need to ask for the consent of individual users.

30.01.2023.