

Privacy Policy

Prohuman Zrt., Service Flow Kft., HR-RENT Kft., HR Montage Kft., ProAktív Közérdekű Nyugdíjas Szövetkezet, PRODIÁK Iskolaszövetkezet, BRC Services Kft., Alkotó Magyarország Nonprofit Kft., Finance Care Hungary Kft., Finance Sales Hungary Kft., Prohuman Innovation Kft. (hereinafter collectively referred to as: Data Controller or Data Controllers) as the operator of the websites available at www.prohuman.hu, www.serviceflow.hu, www.hr-rent.hu, www.hr-group.hu, www.nyugdijasmunka.prohuman.hu, www.prodiak.hu, www.brcservices.hu, www.finance-care.hu, and www.finance-sales.hu (hereinafter collectively referred to as: Website) hereby publish information on data processing carried out in connection with **the Website, services related to the Website, and other services provided** by the Data Controllers.

Given that the purpose of certain data processing activities specified in this Policy and the method of data processing are determined jointly by the Data Controllers, Prohuman Zrt., Service Flow Kft., HR-RENT Kft., HR Montage Kft., ProAktív Közérdekű Nyugdíjas Szövetkezet, PRODIÁK Iskolaszövetkezet, BRC Services Kft., Alkotó Magyarország Nonprofit Kft., Finance Care Hungary Kft., Finance Sales Hungary Kft. Regulation (EU) 2016/679 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 (hereinafter: GDPR) (hereinafter: GDPR) **Chapter IV, Section 1, Article 26, they are considered joint data controllers.**

By using the Website and the services of the Data Controller, visitors to the Website and users of the Data Controller's services (hereinafter referred to as **Users or Data Subjects**) accept all the terms and conditions set out in this Privacy Policy (hereinafter referred to as the **Policy**). Therefore, please read this Policy carefully before using the Website or the services.

1. Details of data controllers

Prohuman Zrt.

Registered office: 1146 Budapest, Hungária krt. 140-144.
Represented by: Göndöcs Viktor and Szeitz Áron
E-mail address: adatvedelem@prohuman.hu

Service Flow Kft.

Registered office: 1134 Budapest, Tüzér utca 39.
Represented by: Finfera Maximilián
E-mail address: adatvedelem@phgroup.hu

HR-RENT Kft.

Registered office: 7624 Pécs, Ferencesek utcája 52.
Represented by: Szeitz Áron and Kutyáncsánin Jevrem
E-mail address: adatvedelem@phgroup.hu

HR-Montage Kft.

Registered office: 7622 Pécs, Ferencesek utcája 52.
Represented by: Scheich Zoltán
E-mail address: adatvedelem@phgroup.hu

ProAktív Közérdekű Nyugdíjas Szövetkezet

Registered office: 1146 Budapest, Hungária körút 140-144.
Represented by: Tóth Rozália and Szeitz Áron
E-mail address: adatvedelem@phgroup.hu

PRODIÁK Iskolaszövetkezet

Registered office: 7624 Pécs, Ferencesek utcája 52.
Represented by: Tóth Rozália and Szeitz Áron
E-mail address: adatvedelem@phgroup.hu

BRC Services Kft.

Registered office: 2724 Újlengyel, Ady Endre utca 41.
Represented by: Zakor Sándor and Szeitz Áron
E-mail address: adatvedelem@phgroup.hu

Alkotó Magyarország Nonprofit Kft

Registered office: 2724 Újlengyel, Kossuth Lajos utca 86.
Represented by: Zakor Sándor and Szeitz Áron
E-mail address: adatvedelem@phgroup.hu

Finance Care Hungary Kft.

Registered office: 1146 Budapest, Hungária krt. 140-144.
Represented by: Jakab Zsolt and Zakor Sándor
E-mail address: adatvedelem@phgroup.hu

Finance Sales Hungary Kft.

Registered office: 1146 Budapest, Hungária krt. 140-144.
Represented by: Jakab Zsolt and Zakor Sándor
E-mail address: adatvedelem@phgroup.hu

Prohuman Innovation Kft.

Registered office: 1146 Budapest, Hungária krt. 140-144.

Represented by:

Szeitz Áron and Fazekas Csaba

E-mail address:

adatvedelem@phgroup.hu

Data Protection Officer:

Dr. Keszey Gábor

adatvedelem@phgroup.hu

Information Security Officer:

Czakó József

informaciobiztonsag@phgroup.hu

2. Scope of data processed

During registration

On the Website and through the registration platform at the Data Controller's offices, the User has the opportunity to provide their data in order to use the services of the Website (hereinafter: **Registration**). During Registration, **the following personal data must be provided** (data marked with * are mandatory):

- full name*,
- e-mail address*,
- password*,
- newsletter subscription.

Users can also register and log in to the Website using their Facebook, Google, or LinkedIn profiles. In this case, with the User's consent, the Website will request the following personal data from the User's profile:

- personal data:
 - address,
 - birth date,
 - nationality,
 - gender,
 - phone number.
- planned place of employment
- type of work
- qualifications
- work experience.

User profile

After registration, the system creates the Data Subject's user profile, which contains the following data:

- the data provided by the Data Subject during Registration,
- the data provided by the Data Subject in connection with job search.

When using the User Profile, the User has the option to upload their CV or create a new CV.

When creating a new CV, the following information can be provided:

- personal data:
 - photo,
 - address,
 - birth date,
 - nationality,
 - gender,
 - phone number;
- qualifications:
 - type of qualification, name, name of institution, date of completion,
 - IT knowledge, certification,
 - language skills: language, level, time of acquisition,
 - type of driver's license, date of issue,
 - other knowledge;
- experience:
 - name of employer,
 - job title,
 - work address,
 - period of employment,
 - job description.

In the User Profile, the User also has the option to enter data related to the job they are looking for (job type, location, other criteria), save job advertisements, modify the data they have entered, delete data (except for non-mandatory data), subscribe to or unsubscribe from newsletters.

Data sheet and interview

The Data Subject also has the option of providing their data, CV, and requirements related to the position to be filled on a paper or digital data sheet (hereinafter: **Data Sheet**) specifically designed for this purpose during **a personal visit to the offices** operated by the Data Controller or during a personal conversation with the Data Controller's advisor (hereinafter: **Interview**), so that the Data Controller can contact them with a suitable job offer. their CV, and their requirements related to the position to

be filled, in order for the Data Controller to contact them with a suitable job offer. When filling out the Data Sheet or during the interview, only the data of the Data Subject that is necessary for job search will be recorded. Based on the data provided on the Data Sheet and during the interview, the Data Controller also creates the Data Subject's User Profile, which may contain the data specified in the "User Profile" section, based on the Data Subject's voluntary consent.

Data collection during telephone consultation

During a telephone conversation with the Data Controller, the Data Subject also has the opportunity to provide their data so that the Data Controller can contact them in the future with job opportunities and send them job offers to the email address they have provided.

- name (first-, and last name)*,
- location,
- phone number,
- e-mail address,
- type of qualification (primary school, vocational school, etc.),
- the type/category of work desired (finance, physical labour, etc.).

Newsletter subscription

On the Website, the Data Subject has the opportunity to subscribe to the Data Controller's newsletter on a specially designated interface. To subscribe to the newsletter, **the following personal data must be provided** (data marked with * are mandatory):

- full name*,
- e-mail address*.

Applying for a job advertisement

The Data Controller processes personal data provided in applications for job offers **advertised on other websites or other advertising platforms** (print media) (CV, identification data, contact details, data related to education, employment, and interests) during and for the purpose of processing the job application. The application process is as follows: the Data Subject sends their data to the Data Controller to the email address indicated in the job advertisement (if the advertisement is displayed by the Data Controller on Facebook, the data of the Data Subjects applying for the advertisement is made available to the Data Controller by Facebook in the form of a downloadable database), the Data Controller confirms the application by email to the email address provided during the application process and sends a questionnaire to the Data Subject in the confirmation email, in which it verifies the data and requests any missing data.

Recording telephone conversations

In the case of data collection during a telephone inquiry, the Data Controller records the telephone conversation and, in doing so, processes the voice of the Data Subject and personal data related to the information disclosed during the conversation.

Upon conclusion of a membership agreement

The Data Controller shall process the Data Subject's data in accordance with the relevant legal provisions, which are essential for the conclusion, performance, and termination of the membership agreement with the Data Controller:

- data specified in the membership agreement:
 - name,
 - birth name,
 - address,
 - date, place of birth
 - mother's (maiden) name,
 - tax identification number,
 - Social Security Number,
 - pension payment reference number,
 - bank account number,
 - phone number,
 - e-mail address;
- data provided in the membership application:
 - name,
 - tax identification number,
 - social security number,
 - bank account number,
 - pension payment reference number,
 - date, place of birth,
 - mother's (maiden) name,
 - permanent address,
 - mail address,
 - e-mail address,
 - phone number,
 - qualifications.

Ad hoc agreement:

- name,

- address
- mother's (maiden) name
- date, place of birth
- tax identification number
- Data related to the fulfilment of the membership agreement:
 - data relating to performance time records,
 - data on vacation and sick leave,
 - income payment data.

When establishing and maintaining an employment relationship for the purpose of temporary agency work

The Data Controller shall process the data of the Data Subject employee in accordance with Section 10 of Act I of 2012 on the Labor Code, which are relevant to the establishment, performance, and termination of the employment relationship with the Data Controller:

- employee identification data:
 - name (birth name),
 - date, place of birth,
 - mother's (maiden) name,
 - nationality,
 - address, place of residence,
 - social security number, tax identification number, ID card number,
 - marital status,
 - number of children, place and date of birth, tax identification number,
 - bank account number,
 - photo;
- data on education and qualifications:
 - data on educational attainment,
 - data related to professional qualifications and certifications,
 - language skills;
- employment-related data:
 - start date of employment, position held, working hours, place of work.
 - the date, manner, and conditions of termination of employment.

The Data Controller shall collect special data only on the basis of the Data Subject's written consent, which is necessary for the performance of the given job (e.g. in the case of the employment or hiring of persons with changed working capacity), or if the Data Subject provides this data themselves and it is not necessary for the performance of the job. The Data Controller shall delete the special data without delay.

Only persons aged 16 or over are entitled to provide data.

3. Purpose of data processing

The data controller uses the data for the following purposes in connection with the services it provides:

- During registration on the Website: the purpose of data processing is to provide the services of the Website and to create a user profile.
- Purpose of data processing when creating a user profile (or filling out the Data Sheet and completing the Interview)
 - management, modification, and deletion of data stored in user profiles and CVs,
 - using the data for the purpose of applying for job advertisements, setting up job searches, saving job offers, and maintaining contact with the User, sending notifications about job offers and job opportunities that match their qualifications, aptitudes, and requirements,
 - processing of data provided during the creation of a CV is to enable the Data Controller to find suitable job offers for the User, as well as to identify the User's qualifications, aptitudes, and requirements that are relevant to the position to be filled,
 - monitoring and promoting the professional development of the Data Subject.
- When subscribing to the newsletter on the Website or in the User Profile: Sending electronic newsletters and advertising messages about offers and prize games related to the Data Controller and its partners to the email address provided by the Data Subject (hereinafter collectively referred to as: **Newsletter**).
- The purpose of data collection during telephone inquiries is to send information about job offers that match the Data Subject's qualifications and interests to the email address provided during the inquiry.
- The purpose of data processing related to the recording of telephone conversations is to record the Data Subject's consent to data processing related to data collection during telephone inquiries for the purpose of retrieving the consent, the content of the communication between the Data Subject and the Data Controller, and the documentation of the Data Controller's information. to document the content of the communication between the Data Subject and the Data Controller, as well as the information provided by the Data Controller. Before starting to record a telephone

conversation, the Data Controller shall in all cases inform the Data Subject that the telephone conversation is being recorded, as well as the purpose of making and storing the audio recording containing personal data, the legal basis for data processing, the duration of storage, the identity of the Data Controller, the persons authorized to access the data, and the provisions of the GDPR concerning the rights of data subjects and the procedure for enforcing them..

- When applying for a job advertisement, the purpose of data processing is o to maintain contact with the Data Subject in relation to the specified job offer; o to forward the Data Subject's data and CV to the employer advertising the specified job offer, based on the Data Subject's consent
 - conducting the selection process related to the job advertisement published by the Data Controller,
 - facilitating the establishment and maintenance of employment relationships,
 - with separate consent, creating a user profile for the Data Subject, identifying the Data Subject's qualifications, aptitudes, and needs that are relevant to the employment relationship to be filled; providing the Data Subject with job offers that match their interests, qualifications, aptitudes, and needs.
- In the event of membership, the purpose of data processing is to fulfil, maintain, and terminate the membership relationship between the Data Controller and the Data Subject, in particular the performance of administrative tasks related to the performance of tasks (including personnel tasks, income calculation, transfer and social security settlements) and HR controlling (including the efficient business organization of human resources). Based on the Data Subject's express and voluntary consent, the Data Controller shall transfer the Data Subject's personal data to a third party (the Service User) specified in the individual agreement on the performance of tasks related to the membership agreement for the purpose of data processing in the framework of the cooperative membership relationship, to the extent necessary for this purpose..
- When establishing and maintaining an employment relationship for the purpose of temporary agency work, the purpose of data processing is to establish an employment relationship between the Data Controller and the Data Subject employee, the performance of the employment relationship, and the exercise of rights and fulfilment of obligations arising from the employment relationship in connection with the termination of the employment relationship, in accordance with the provisions of the employment contract and the provisions of the Labor Code - with particular regard to Section 10 of the Labor Code.

The Data Controller also uses the personal data provided by the User for statistical purposes, exclusively in such a way that the personal data is anonymized, so that it is no longer suitable for identification and cannot be linked to any natural person.

4. Duration of data processing

The Data Controller shall process personal data for the duration of the purpose of data processing, i.e. in connection with registration on the Website, in the case of User profiles, in connection with data collection during telephone enquiries, and in the case of sending Newsletters, until the User requests the deletion of their data or withdraws their consent to the processing of their personal data or to receiving Newsletters.

The Data Controller shall retain the recording made during the telephone conversation and the personal data recorded on the recording for the purpose of data processing related to data collection during the telephone inquiry until the consent is withdrawn (or until a request for deletion of the data covered by the consent is made). If the Data Subject does not consent to the processing of their data for the purpose of data collection during the telephone inquiry, the Data Controller shall delete the audio recording immediately after the end of the telephone conversation.

Personal data shall be deleted at the same time as the purpose of data processing ceases to exist, or at the User's request without undue delay, except for data which the Data Controller is required to retain for the period specified in the legislation prescribing mandatory data processing on the basis of a legal obligation, thus, the Data Controller shall retain personal data processed in the course of establishing, , until the expiry of the limitation period for labor law claims arising from the employment relationship, i.e. for 3 years from the termination of the employment relationship pursuant to Section 286 (1) of the Labor Code, or, if the law prescribes a longer period, for that period.

In the event of membership, the Data Controller shall process personal data for the duration of the purpose of data processing. In the event of termination of membership, the Data Controller shall delete personal data one year after the termination of membership. In the case of mandatory (legally based) data processing, the Data Controller shall process the data for the period specified in the legislation.

When applying for a job advertisement, the Data Controller shall process personal data for the duration of the purpose of data processing, i.e. in the case of a specific job offer, until the time of processing related to the job offer, and in the case of forwarding a job offer that matches the Data Subject's interest or choice, for as long as the purpose of data processing exists, or until the Data Subject requests the deletion of their data or withdraws their consent.

5. Data transfer

In order to perform the services it provides, when applying for a specific job advertisement, the Data Controller shall transfer the data necessary for the assessment of the application – personal data, studies, work experience, other information necessary for the assessment of the application (planned start date, test results, etc.) – to the

employer who advertised the job specified in the job advertisement (hereinafter: **Employer**).

In the case of any data transfer where the recipient of the transfer is an Employer conducting data processing activities in a third country, the Data Controller shall only transfer the User's personal data if the User has been duly informed in advance and has given their express consent.

The Data Controller declares that, following the transfer of data to the Employer, it shall not be held liable for the lawfulness of the Employer's processing of such data. The Data Subject may obtain information regarding the Employer's data processing on the Employer's website or through other means of contact.

6. Legal basis for the processing of personal data

In connection with registration, use of the user profile, application for job advertisements, subscription to the newsletter, and data collection during telephone inquiries, the Data Subject consents to the Data Controller processing their personal data as described in this Policy. The processing of personal data is based on the voluntary consent of the Data Subject, given in full knowledge of this Policy.

The legal basis for data processing related to the recording of telephone conversations is the legitimate interest of the Data Controller, which is based on Article 6(1)(f) of the GDPR. In order to comply with the referenced provision, the Data Controller performed a balancing test, as a result of which it determined the following:

- The Data Controller - in its opinion - has a legitimate interest in documenting and proving the communication that takes place during the telephone conversation, the consent given by the Data Subject for the purposes of data processing specified in point a), as well as the information provided by the Data Controller during the telephone conversation, in order to ensure the traceability of the consent and communication.
- The purpose of data processing is to record the Data Subject's consent given for the data processing specified in point a) for the purpose of retrieving the consent, to document the identity of the Data Subject, the content of the communication between the Data Subject and the Data Controller, and the information provided by the Data Controller for the purpose of enforcing the legitimate interests of the Data Controller.
- The data controller may use the personal data recorded during the audio recording exclusively in connection with the handling of complaints or inquiries arising in relation to the data subject concerned, or as evidence in court or administrative proceedings.
- The Data Controller's legitimate interest as defined in this section and data processing based on legitimate interest proportionally restrict the Data Subject's right to the protection of their personal data and private life. The Data Controller

has examined all the means and possibilities available to it from the point of view of legitimate interest and data processing in order to achieve the desired goal specified in this Policy , and has concluded that the use of audio recording in the manner specified in this Policy is the solution that restricts privacy the least and thus meets the requirements of necessity and proportionality. To this end

- After the retention period specified in the information notice has expired, the audio recordings will be deleted automatically and without delay,
- The Data Controller may use the recorded data exclusively for the purposes specified in this Policy,
- The Data Controller has determined the retention period for the recordings with a view to ensuring that it is appropriate for the purpose specified in this notice and that it is suitable for achieving that purpose. In the opinion of the Data Controller, the retention period specified in this Policy is justified because this period adequately ensures that, if necessary, the recordings are available as evidence for the purposes of verifying the existence of consent, handling any complaints, or in the event of any administrative or judicial proceedings,
- The Data Controller complies with legal obligations in all cases,
- The Data Controller shall ensure that Data Subjects are able to exercise their rights as set out in this Policy under all circumstances, in particular the right to object.

Based on the above, the Data Controller considers that the data processing related to the recording of telephone conversations complies with the legal and regulatory requirements for data processing based on legitimate interests.

The Data Subject may only provide their own personal data on the Website or when using the Data Controller's services.

7. Data security

The Data Controller undertakes to ensure the security of the data, to take the technical and organizational measures and to establish the procedural rules necessary to ensure that the data collected, stored and processed are protected and to prevent their destruction, unauthorized use and unauthorized alteration. The Data Processor also undertakes to require any third parties to whom it transfers or discloses data with the consent of the Data Subjects to comply with data security requirements.

The Data Controller shall ensure that no unauthorized person may access, disclose, transfer, modify, or delete the processed data. The processed data may only be accessed by the Data Controller, its employees, and the Data Processor(s) used by it, and the Data Controller shall not transfer the data to third parties who are not authorized to access the data.

The Data Controller shall do everything in its power to prevent accidental damage or destruction of the data. The Data Controller shall impose the above obligation on its employees involved in data processing activities.

The Data Subject acknowledges and accepts that when providing personal data on the Website, despite the fact that the Data Controller has modern security measures in place to prevent unauthorized access to or disclosure of data, the protection of data cannot be fully guaranteed on the Internet. In the event of unauthorized access or disclosure of data despite our efforts, the Data Controller shall not be liable for such data acquisition or unauthorized access or for any damage incurred by the Data Subject for these reasons. In addition, the Data Subject may also provide their personal data to third parties who may use it for unlawful purposes or in an unlawful manner.

The Data Controller shall ensure data security using the most up-to-date methods available. The Data Controller undertakes to immediately suspend the service and publish a statement until the error is rectified in the event of data protection incidents occurring despite the measures set out above, and to keep a record of data protection incidents and the measures taken.

8. Persons authorized to access personal data, data processing

The Data Controller and those Employers to whom the Data Subject has expressly consented to the transfer of their personal data are entitled to access the Data Subject's data.

Data Processors used by the Data Controller to access personal data are entitled to do so in accordance with applicable law.

Data processing is carried out by the following data processors acting on behalf of the Data Controller:

- DoclerNet Hosting Kft. (1023, Budapest, Lajos u. 28-32): hosting service
- Prohuman Zrt. (1146, Budapest, Hungária krt. 140-144.): system development
- Gbart Solutions Kft. (1173 Budapest, Pesti út 17.): website management
- Textkernel BV. (Nieuwendammerkade 26A-5, 1022 AB): IT services related to database use
- INPHONE Adatfeldolgozó és Információs Szolgáltató Kft. (1118 Budapest, Rétköz u. 5.; Cg.: 01-09-562494)
- NEXON Kft. (1138, Budapest, Váci út 185.): accounting and payroll services related to database use

The Data Controller reserves the right to involve additional data processors in data processing in the future, about which it will inform Users by amending this Policy.

In the absence of express legal provisions, the Data Controller will only transfer data suitable for personal identification to third parties with the express consent of the User concerned.

9. The rights of the data subject in relation to their processed data

9.1 Right of access

At the User's request, the Data Controller shall provide information on whether the Data Controller processes personal data relating to the User and, if so, shall grant access to the personal data and provide the following information:

- the purpose(s) of data processing,
- the types of personal data involved in data processing,
- in the event of the transfer of the User's personal data, the legal basis for the transfer and the recipient(s),
- the planned duration of data processing,
- the User's rights in relation to the rectification, erasure, and restriction of processing of personal data, as well as the right to object to the processing of personal data,
- the possibility of appealing to the Authority,
- source of data,
- the name, address, and data processing activities of data processors.

The Data Controller shall provide the User with a copy of the personal data subject to data processing free of charge. The Data Controller may charge a reasonable fee based on administrative costs for any additional copies requested by the User. If the User has submitted the request electronically, the information shall be provided in a widely used electronic format, unless the data subject requests otherwise.

The Data Controller shall provide the information in an easily understandable form, without undue delay, but no later than 30 days from the date of submission of the request, at the request of the User. The User may submit their request for access by email to adatvedelem@phgroup.hu or by post to the following address: 1146 Budapest, Hungária krt. 140-144. In both cases, proof of identity must be provided.

In connection with the audio recording made during the telephone conversation, the Data Subject may request that the Data Controller inform them in writing about the content of the recording. In the course of providing this information, the Data Controller shall inform the Data Subject about the exact content of the audio recording made in connection with them. The Data Controller shall respond in writing within one month of receiving the request. The Data Subject also has the opportunity to listen to the recorded conversation containing his or her personal data but is not entitled to request a copy of the recorded conversation. In connection with the playback, the Data Controller shall in all cases prepare the minutes specified in Annex 1 to this Policy. The minutes shall be kept by the Data Controller for 3 years.

9.2 Correction of processed data

Users are entitled to request the correction of inaccurate personal data or the completion of incomplete data (indicating the correct data) taking into account the purpose of data processing, also at the email address adatvedelem@phgroup.hu or at the postal address 1146 Budapest, Hungária krt. 140-144. postal address, in both cases with proof of identity. The data controller shall make the correction in its records without undue delay and notify the data subject in writing that this has been done. Within the scope of the right to rectification, the data subject may request the modification of certain data recorded in connection with the audio recording of the telephone conversation (e.g. correction of the date of the audio recording), provided that he or she can prove that the data does not correspond to reality.

9.3 Deletion of processed data (right to be forgotten)

In addition to the above, users may request the deletion of their data at any time, in whole or in part, by sending an email to adatvedelem@phgroup.hu or by post to 1146 Budapest, Hungária krt. 140-144, free of charge and without justification, upon verification of their identity, if any of the following reasons apply:

- a) the personal data is no longer necessary for the purposes for which it was collected or otherwise processed,
- b) the User withdraws their consent and there is no other legal basis for data processing,
- c) the User objects to the processing of his or her personal data,
- d) the processing of personal data was unlawful,
- e) personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the controller is subject,
- f) the collection of personal data based on consent took place in connection with the provision of information society services to children.

If the Data Controller has disclosed personal data and is obliged to delete it on the basis of the above, it shall take reasonable steps, taking into account available technology and implementation costs, to inform data controllers processing the personal data concerned that the User has requested them to delete links to, or copies or replicas of, the personal data in question.

Personal data does not need to be deleted if data processing is necessary:

- for the purpose of exercising freedom of expression and the right to information,
- compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried

out in the public interest or in the exercise of official authority vested in the controller,

- on grounds of public interest relating to public health,
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, insofar as the right to erasure is likely to render impossible or seriously impair such processing, or
- to submit, enforce, and defend legal claims.

The data subject shall only be entitled to request the deletion of the audio recording made during the telephone conversation after the specified retention period and only if the recording has not yet been destroyed by the Data Controller and the deletion is not precluded by any legal provision.

9.4 Restriction of processed data

The User shall have the right to request that the Data Controller restrict the processing of personal data instead of rectifying or erasing it, if any of the following conditions are met:

- the User disputes the accuracy of the personal data, in which case the restriction applies for a period enabling the controller to verify the accuracy of the personal data,
- the data processing is unlawful and the User opposes the erasure of the data and requests the restriction of their use instead,
- the Data Controller no longer needs the personal data for data processing purposes, but the User requires them for the submission, enforcement, or defense of legal claims, or
- the User has objected to the processing of the data; in this case, the restriction applies for the period until it is determined whether the legitimate grounds of the data controller take precedence over the legitimate grounds of the data subject.

If data processing is restricted, such personal data may only be processed, with the exception of storage, with the consent of the User, or for the establishment, exercise, or defense of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.

The Data Controller shall inform the User whose data processing has been restricted at their request in advance of the lifting of the restriction on data processing.

9.5 Notification obligation regarding the rectification or erasure of personal data or the restriction of processing

The Data Controller shall inform all recipients to whom personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves a disproportionate effort. At the request of the User, the Data Controller shall inform the Data Controller of these recipients.

The Data Subject may also decide at any time that the Data Controller should no longer send them Newsletters. The Data Subject may withdraw their consent to receive Newsletters at any time, free of charge, without justification or restriction, by clicking on the unsubscribe link at the bottom of the newsletters, or by sending a letter to adatvedelem@phgroup.hu or 1146 Budapest, Hungária krt. 140-144. (including their exact personal details). Upon receipt of the unsubscribe request, the Data Controller shall immediately delete the unsubscribing Data Subject's data from its direct marketing database and shall no longer send Newsletters to the Data Subject.

If the withdrawal of consent only affects data processing for direct marketing purposes (sending newsletters), the Data Controller shall immediately delete the Data Subject from the direct marketing register, but shall otherwise remain entitled to process the Data Subject's data in order to provide the Website services used by the Data Subject.

9.6 Right to protest

The User may object to the processing of their personal data if the data processing

- necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller,
- necessary for the enforcement of the legitimate interests of the Data Controller or a third party.

In the event of an objection by the User, the Data Controller may no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the User or for the establishment, exercise, or defense of legal claims.

If personal data is processed for direct marketing purposes, the User has the right to object at any time to the processing of personal data concerning them for such purposes. If the User objects to the processing of personal data for direct marketing purposes, the personal data shall no longer be processed for such purposes.

In connection with data processing during the recording of telephone conversations, the Data Subject may object to the processing of their personal data if the Data Controller uses the personal data contained in the recording for purposes other than those specified in this Policy. If the Data Subject objects to the processing of personal data for a different purpose, the personal data may no longer be processed for that purpose.

9.7 Data Controller's action in connection with the Data Subject's request

The Data Controller shall inform the User without undue delay, but no later than one month after receipt of the request, of the measures taken in response to the request for access, rectification, erasure, restriction, objection, and data portability. If necessary, taking into account the complexity of the request and the number of requests, this deadline may be extended by a further two months. The Data Controller shall inform the User of the extension of the deadline within one month of receipt of the request, indicating the reasons for the delay. If the User submitted the request electronically, the information shall be provided electronically, unless the data subject requests otherwise.

If the Data Controller does not take action on the User's request, it shall inform the User without delay, but no later than one month after receiving the request, of the reasons for not taking action and that the User may lodge a complaint with a supervisory authority and exercise their right to judicial remedy.

Upon the User's request, the information, notification, and action taken on the basis of the request shall be provided free of charge. If the User's request is clearly unfounded or excessive, in particular due to its repetitive nature, the Data Controller may charge a reasonable fee or refuse to take action on the request, taking into account the administrative costs of providing the requested information or communication or taking the requested action. The burden of proving that the request is manifestly unfounded or excessive lies with the Data Controller.

10. Data security

The Data Controller undertakes to ensure the security of the data, to take the technical and organizational measures and to establish the procedural rules necessary to ensure that the data collected, stored and processed are protected and to prevent their destruction, unauthorized use and unauthorized alteration. The Data Processor also undertakes to require any third parties to whom it transfers or discloses data with the consent of the Data Subject to comply with data security requirements.

The Data Controller shall ensure that no unauthorized person may access, disclose, transfer, modify, or delete the processed data. The processed data may only be accessed by the Data Controller, its employees, and the Data Processor used by it; the Data Controller shall not transfer the data to third parties who are not authorized to access the data.

The Data Controller shall do everything in its power to prevent accidental damage to or destruction of the data. The Data Controller shall impose the above obligation on its employees involved in data processing activities.

Recordings made during telephone conversations shall be stored by the data processor in a closed server room certified in accordance with the ISO/IEC 27001 international standard for information security management.

11. Handling and reporting data protection incidents

A data protection incident is any event that, in relation to personal data processed, transmitted, stored, or processed by the Data Controller, involves the unlawful processing or processing of personal data, in particular unauthorized or accidental access, alteration, disclosure, erasure, loss or destruction, as well as accidental destruction and damage.

The Data Controller shall, without undue delay, but no later than 72 hours after becoming aware of the data protection incident, unless the Data Controller can demonstrate that the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification cannot be made within 72 hours, the reason for the delay must be indicated, and the required information may be provided in instalments without further undue delay. The notification to the NAIH shall contain at least the following information:

- the nature of the data breach, the number and categories of data subjects and personal data involved,
- Name and contact details of the data controller,
- the likely consequences of the data protection incident,
- measures taken or planned to manage, prevent, and remedy the data breach.

The Data Controller shall inform the data subjects of the data protection incident within 72 hours of its detection via the Data Controller's website. The information shall include at least the data specified in this section.

The Data Controller shall keep a record of data protection incidents for the purpose of monitoring measures related to data protection incidents and informing data subjects. The record shall contain the following data:

- the scope of personal data concerned,
- the scope and number of persons concerned,
- date of the data breach,
- the circumstances and effects of the data protection incident,
- measures taken to remedy the data protection incident.

The Data Controller shall retain the data contained in the register for 5 years from the date of detection of the data breach.

12. Legal remedies

The Data Controller shall make every effort to ensure that personal data is processed in accordance with the law, but if the Data Subject feels that this has not been done, they may write to adatvedelem@phgroup.hu or to the postal address 1146 Budapest, Hungária Krt. 140-144.

If the Data Subject feels that their right to the protection of personal data has been violated, they may seek legal remedy from the competent authorities in accordance with the applicable laws:

- National Data Protection and Freedom of Information Authority (1055 Budapest, Falk Miksa utca 9-11.; ugyfelszolgalat@naih.hu; www.naih.hu)
- in court.

The National Media and Communications Authority is responsible for advertising sent electronically (newsletters), Detailed regulations can be found in Act CXII of 2011 on the right to self-determination in information and freedom of information, as well as in Act CVIII of 2001 on certain issues related to electronic commerce services and information society services.

13. Other provisions

This Policy is governed by Hungarian law and the provisions of the GDPR.