Privacy Policy

The purpose of this Data Management Information Sheet (hereinafter: Information Sheet) is to provide the interested parties with adequate information about the personal data managed by the LifeMax Association (hereinafter: Data Controller), their source, the purpose, legal basis, and duration of the data processing, as well as the name and address of the data processor involved in the data processing. and activities related to data management, the legal basis and recipient of data transmission in the case of forwarding the data subject's personal data, as well as the data subject's rights.

The basic purpose of the Notice is for the Data Controller to ensure the protection of personal data during the processes and procedures associated with the management of personal data arising in connection with its activities. Regulation No. 2016/679 on the flow and repeal of Regulation 95/46/EC (hereinafter: GDPR), as well as Regulation CXII of 2011 on the right to information self-determination and freedom of information. according to law (hereinafter: Isdafoi.).

The Information is GDPR and Isdafoi. It is based on point a) of § 14 and paragraph (1) of § 16, according to which the Data Controller is obliged to inform the data subject clearly and in detail about all the facts related to the processing of his personal data before the start of data processing.

The Data Controller acknowledges the contents of this Notice as binding on itself and undertakes to ensure that all data processing related to its activities meets the requirements set out in the Notice and applicable laws.

1) Data of the data controller

Name: LifeMax Association

Headquarters: Hungary 4028 Debrecen, Simonyi street 14.

Representative: Tamas Winter

Tax number: 18840227-2-09

Court registration number: 16-02-0002122

Telephone number: +443300272192

Name and contact information of the data protection officer: Dr. Zoltán Kiss-Kósa, drkisszoli84@gmail.com,

2) TERM EXPLANATION

Regarding the interpretative provisions, the GDPR. and Isdafoi. its provisions shall govern.

Data subject: natural person identified or identifiable on the basis of any information.

Personal data: any information relating to the data subject. A natural person can be identified directly or indirectly, in particular on the basis of an identifier such as a name, number, location data, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person can be identified.

Special data: all data belonging to special categories of personal data, i.e. personal data referring to racial or ethnic origin, political opinion, religious or worldview beliefs or trade union membership, as well as genetic data, biometric data aimed at unique identification of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons.

Genetic data: all personal data relating to the inherited or acquired genetic characteristics of a natural person, which carries unique information about the physiology or state of health of the given person, and which primarily results from the analysis of a biological sample taken from the given natural person.

Biometric data: personal data related to the physical, physiological or behavioral characteristics of a natural person, obtained through specific technical procedures, which enable or confirm the unique identification of a natural person, such as a facial image or dactyloscopic data.

Health data: personal data relating to the physical or mental state of health of a natural person, including data relating to the health services provided to the natural person, which carries information about the state of health of the natural person.

Data of public interest: information or knowledge in the management of a body or person performing a state or local government task, as well as other public tasks defined by law, related to its activities or generated in connection with the performance of its public tasks, which does not fall under the concept of personal data, recorded in any way or form, regardless of the way it is handled , from its independent or collective nature, so in particular data relating to powers, jurisdiction, organizational structure, professional activity, including its effectiveness, the types of data held and the laws governing the operation, as well as management, concluded contracts.

Data that is public in the public interest: any data that does not fall under the concept of data in the public interest, the disclosure, disclosure or making available of which is ordered by law in the public interest.

Consent: the voluntary, definite and clear declaration of the will of the data subject based on adequate information, with which the data subject indicates, through a statement or other behavior that clearly expresses his will, that he gives his consent to the processing of his personal data.

Data controller: the natural or legal person or organization without legal personality who, within the framework defined by law or a mandatory legal act of the European Union, independently or together with others determines the purpose of data management, the data management (including the device used) makes and implements relevant decisions, or has them implemented by the data processor.

Data management: regardless of the procedure used, any operation performed on the data or the set of operations, including in particular collection, recording, recording, organizing, storing, changing, using, querying, transmitting, disclosing, harmonizing or connecting, locking, deleting and destroying, and preventing further use of the data, taking photographs, audio or video recordings, and recording

physical characteristics suitable for identifying the person (e.g. fingerprint or palm print, DNA sample, iris image).

Data processor: a natural or legal person, or an organization without legal personality, who - within the framework and conditions defined by law or a mandatory legal act of the European Union - processes personal data on behalf of or at the direction of the data controller.

Data processing: the set of data processing operations performed by a data processor acting on behalf of or at the request of the data controller.

Data transmission: making the data available to a specific third party.

Recipient: the natural or legal person or organization without legal personality to whom or to whom personal data is made available by the data controller or data processor.

Data destruction: complete physical destruction of the data carrier containing the data.

Third party: a natural or legal person, or an organization without legal personality, who is or is not the same as the data subject, the data controller, the data processor or the persons who carry out operations aimed at processing personal data under the direct control of the data controller or data processor.

If the definitions of concepts in the current data protection legislation differ from the interpretative provisions of this Information, then the concepts defined by the current legislation are the governing ones.

3) PRINCIPLES OF DATA MANAGEMENT

Informational self-determination is the fundamental right of every natural person laid down in the Basic Law, so the Data Controller performs data processing only and exclusively in accordance with the provisions of the applicable legislation, thus in particular observing the following basic principles:

Principle of legality, fair procedure and transparency: The Data Controller handles personal data legally and fairly, as well as in a transparent manner for the data subject.

Purpose-bound principle: Personal data is collected only for a specific, clear and legitimate purpose, and the Data Controller does not handle it in a way that is incompatible with these purposes.

Principle of data economy: In order to maintain the principle of data economy, the Data Controller may only process personal data that is appropriate and relevant for the purposes of data management, and is limited to the necessary extent.

Principle of accuracy: The Data Controller ensures the accuracy, completeness, inviolability, confidentiality and up-to-dateness of personal data, as well as that the data subject can only be identified for the time necessary for the purpose of data management.

Principle of limited storage: Personal data is stored in a form that allows the identification of the data subjects only for the time necessary to achieve the goals of personal data management.

"Integrity and confidentiality" principle: Personal data is handled by the Data Controller in such a way that adequate security of personal data is ensured by applying appropriate technical or organizational

measures, including protection against unauthorized or illegal processing, accidental loss, destruction or damage of data.

Principle of accountability: The Data Controller is responsible for compliance with the relevant basic principles of personal data, as well as for the verifiability of this compliance.

Built-in and default data protection principle: A conscious way of thinking according to which, both when determining the method of data management and during data management (even before it begins), the Data Controller implements appropriate technical and organizational measures with the aim of effectively implementing the above principles and fulfilling obligations, and it does all of this in a regulated and documented manner.

4) PURPOSE OF DATA MANAGEMENT

The GDPR and Isdafoi. pursuant to its provisions, the Data Controller may only process personal data for a specific purpose, in order to exercise a right and fulfill an obligation, which personal data may only be processed to the extent and for the duration necessary for the realization of the purpose. At the Data Controller, personal data is collected and handled fairly and in accordance with the relevant legal regulations, legally. The Data Controller only manages personal data that is essential for the realization of the purpose of data management and thus suitable for achieving the purpose.

5) LEGAL BASIS FOR DATA PROCESSING IN GENERAL

The GDPR and Isdafoi. according to its provisions, the processing of personal data is legal if at least one of the following is fulfilled:

The data subject has given his consent to the processing of his personal data. (GDPR Article 6 (1) point a)

The processing of personal data is necessary for the performance of a contract to which the data subject is a party. (GDPR Article 6 (1) point b)

Data management is necessary to fulfill the legal obligation of the data controller. (GDPR Article 6 (1) point c)

Data management is necessary to protect the vital interests of the data subject. (GDPR Article 6 (1) point d)

Data management is necessary to perform a task of public interest. (GDPR Article 6 (1) point e)

It is necessary to enforce the legitimate interests of the data controller or a third party. (GDPR Article 6 (1) point f)

6) SCOPE OF MANAGED DATA

LifeMax's main activities related to data management are as follows:

concluding contract,

contract performance (service provision),

Dispatch Center data management,

marketing communication, public information, recall at the request of the data subject,

send a newsletter,

data management related to labor and personnel records,

data management related to applications, CVs - workforce management,

data management related to the insurance relationship/personal discount statement,

data management related to the declaration of family tax relief,

data management related to working time records,

handling of special data.

6.1) DATA PROCESSING RELATED TO CONCLUSION OF CONTRACT

The purpose of data management:

Conclusion of a contract, which can take place: electronically, by telephone, in person.

Legal basis for data management:

GDPR Article 6 (1) point b): data processing is necessary to fulfill a contract to which the data subject is a party, or it is necessary to take steps at the request of the data subject prior to the conclusion of the contract.

Scope of processed data:

Name, place of birth, date of birth, address, telephone number, e-mail address of the person concerned.

Duration of data management:

During the duration of the contract, and after the termination of the agreement, until the end of the limitation period open for asserting a legal claim.

The retention period of financial documents related to the performance of the service (e.g. invoices) is a maximum of 8 years in order to ensure tax self-audit. After this, we delete or scrap and destroy the receipts.

6.2) FOR CONTRACT PERFORMANCE - SERVICE PROVISION - RELATED DATA MANAGEMENT

Based on the consent of the data subject, the Data Controller manages the personal data of those who have contracted with it for the purpose of concluding, fulfilling, registering, terminating, avoiding future legal disputes, and maintaining contact with the partner.

The purpose of data management:

Fulfillment of the contract, provision of services, customer relations.

Legal basis for data management:

GDPR Article 6 (1) point a): the data subject has given his consent to the processing of his personal data for one or more specific purposes.

Regarding special data: Article 9 (2) GDPR.

Scope of processed data:

In the case of a beneficiary/beneficiary: name, place of birth, date of birth, address, telephone number, e-mail address, NI number, description of diseases, blood type, height, weight, medications taken, drug sensitivity, allergies, sports, exercise, leisure activities.

In the case of persons to be notified and/or relatives: name, telephone number, type of relationship (e.g.: child, neighbor, etc.).

Duration of data management:

During the duration of the contract, and after the termination of the agreement, until the end of the limitation period open for asserting a legal claim.

The retention period for financial documents related to the performance of the service (e.g. invoices) is a maximum of 5 years in order to ensure tax self-audit. After this, we delete or scrap and destroy the receipts.

6.3) DATA MANAGEMENT OF CONVERSATIONS AND ARRANGEMENTS CONTINUED THROUGH THE DISPATCH CENTER

The purpose of data management:

Informing stakeholders regarding questions, requests, and comments made during contact; retrievability and verification of the exchange of information during the contact. Management of health data appearing in the LifeMax SoulBuddy application and, if necessary, forwarding it to the health care provider providing emergency health care services.

Legal basis for data management:

Consent of the data subject - Article 6 (1) GDPR point a): the data subject has given his consent to the processing and transmission of his personal data for one or more specific purposes to the healthcare provider providing emergency care.

Scope of processed data:

During the use of the Dispatch Center, conversations with customers are recorded, and personal data may also be recorded in the audio (for example, name, mailing address, telephone number, e-mail

address). At the beginning of the telephone conversation, the customer declares whether he consents to the recording of the conversation. If so, the verbal consent will also be recorded together with the audio recording.

If the customer does not consent to the recording of the audio recording, the audio recording will not be recorded. In this case, administration can no longer be carried out over the phone, so the person concerned cannot use the services of the Dispatch Center, and an alternative method of administration (e.g. personal administration) will be offered to him.

Instant health data such as heart rate, body temperature, blood pressure sent during automatic signaling of the LifeMax application.

Duration of data management:

If the customer has given their consent to the recording, 5 years from the date of connection.

If you do not consent to the recording, your personal data will be deleted immediately.

In the case of an emergency call, the legal claim enforcement period is 5 years from the date the call was initiated.

6.4) MARKETING COMMUNICATION, PUBLIC INFORMATION, RECALL AT THE REQUEST OF THE PARTICIPANT

The purpose of data management:

Informing the population for the purpose of marketing communication, as well as calling back following contact initiated by the stakeholders. The purpose of recording phone calls is for accurate administration, as well as the subsequent retrievability and verification of what was said in the conversation.

Legal basis for data management:

Consent of the data subject - Article 6 (1) GDPR point a): the data subject has given his consent to the processing of his personal data for one or more specific purposes.

Scope of processed data:

The name, address, telephone number and e-mail address of the person concerned.

At the beginning of the telephone conversation, the customer declares whether he consents to the recording of the conversation. If so, the verbal consent will also be recorded together with the audio recording.

If the customer does not consent to the recording of the audio recording, the audio recording will not be recorded. In this case, administration can no longer be carried out over the phone, so the person concerned cannot use the services of the Dispatch Center, and an alternative method of administration (e.g. personal administration) will be offered to him.

Duration of data management:

5 years from the date of joining.

6.5) SENDING NEWSLETTER

The purpose of data management:

Informing the affected parties about the services provided by the Data Controller.

Legal basis for data management:

Consent of the data subject - Article 6 (1) GDPR point a): the data subject has given his consent to the processing of his personal data for one or more specific purposes.

Scope of processed data:

The name and e-mail address of the person concerned.

Duration of data management:

Until unsubscribing from the newsletter.

6.6) DATA MANAGEMENT RELATED TO EMPLOYMENT AND PERSONNEL REGISTRATION

The purpose of data management:

Management of labor and personnel records and keeping them up-to-date.

Legal basis for data management:

Legal authorization (Act I of 2012 on the Labor Code) - Article 6 (1) point c) of the GDPR, and data subject consent - Article 6 (1) point a) of the GDPR.

Name, birth name, place and time of birth of the person concerned, mother's name, address, residential address, mailing address, nationality, tax identification number, social security number, pensioner's identification number (in the case of a retired employee), telephone number, e-mail address, identity card number, number of official address card, bank account number, online identifier (if applicable), starting and ending date of employment, job title, copy of document certifying education or professional qualifications, photograph, CV, amount of salary, data related to salary payment and other benefits, from the employee's salary the debt to be deducted based on a legally binding decision or legislation, or your written consent, and the right to this, the manner and reasons for the termination of the employment relationship, proof of professional experience, your moral certificate depending on the position, the summary of the suitability tests for the job, the name of the fund in the case of private pension fund and voluntary mutual insurance fund membership, identification number and membership number of the employee, passport number in the case of a foreign employee; the name and number of the document certifying the right to work.

Duration of data management:

5 years after the termination of the employment relationship, with the exception of the documents proving the legal relationship necessary for the establishment of pension benefits, which the Data Controller must keep for five years after reaching the old-age pension age applicable to the insured or former insured.

6.7) DATA MANAGEMENT RELATED TO APPLICATIONS, RESUMES - WORKFORCE MANAGEMENT

The purpose of data management:

Filling advertised positions, managing the data of applicants, as well as data management related to applications and resumes.

Legal basis for data management:

Data subject consent GDPR Article 6 (1) para. based on point a).

Scope of processed data:

Name, place of birth, date of birth, mother's name, address, qualification documents, photograph, telephone number, e-mail address of the person concerned.

Duration of data management:

Until the application is evaluated. The data of applicants who are not selected will be deleted.

6.8) DATA MANAGEMENT RELATED TO INSURANCE LEGAL RELATIONSHIP AND PERSONAL BENEFIT STATEMENT

The purpose of data management:

Fulfillment of obligations prescribed by legislation, notification of insurance relationship, validation of personal discount.

Legal basis for data management:

Legal authorization (Act LXXX of 1997 on those entitled to social security benefits and private pensions and the coverage of these services) - Article 6(1)(c) GDPR.

Scope of processed data:

Name, place and time of birth of the person concerned, mother's name, NI number, tax identification number, number of working hours, nature of employment, BNO code.

Duration of data management:

5 years after the termination of the employment relationship, with the exception of the documents proving the legal relationship necessary for the establishment of pension benefits, which the Data Controller must keep for five years after reaching the old-age pension age applicable to the insured or former insured.

Recipient of data transmission:

Hungarian State Treasury and the National Tax and Customs Office.

6.9) DATA MANAGEMENT RELATED TO FAMILY TAX BENEFIT DECLARATION

The purpose of data management:

Fulfillment of obligations prescribed by law, enforcement of family tax relief.

Legal basis for data management:

Legal authorization (Act LXXX of 1997 on those entitled to social security benefits and private pensions and the coverage of these services) - Article 6(1)(c) GDPR.

Scope of processed data:

Name, place and time of birth of the person concerned, mother's name, address, tax identification number, personal data of dependents.

Duration of data management:

5 years after the termination of the employment relationship, with the exception of the documents proving the legal relationship necessary for the establishment of pension benefits, which the Data Controller must keep for five years after reaching the old-age pension age applicable to the insured or former insured.

Recipient of data transmission:

Hungarian State Treasury and the National Tax and Customs Office.

6.10) DATA MANAGEMENT RELATED TO WORKING TIME REGISTRATION

The purpose of data management:

Fulfillment of obligations prescribed by legislation, regular registration of working hours.

Legal basis for data management:

Legal authorization (Act I of 2012 on the Labor Code) - Article 6 (1) point c) GDPR, as well as the data subject's consent Article 6 (1) GDPR. based on point a).

Scope of processed data:

Name and signature of the person concerned, beginning and end of working hours.

Duration of data management:

Until the end of the limitation period open for asserting a legal claim, five years after the payment of wages.

6.11) HANDLING OF SPECIAL DATA

Specifying special categories of personal data - neither in whole nor in part - is optional. Special data may only be processed in order to ensure the service and improve its effectiveness, based on the consent of the data subject.

The purpose of data management:

If it becomes necessary during the provision of the service, the Data Controller's dispatcher can hand over the data to the medical service, ambulances, or other healthcare professionals, thus speeding up and facilitating their procedures.

Legal basis for data management:

Article 6(1)(a) GDPR: the data subject has given his consent to the processing of his personal data for one or more specific purposes

Regarding special data: Article 9 (2) GDPR.

Scope of processed data:

Name, place of birth, date of birth, address, telephone number, e-mail address, Taj number, description of diseases, blood type, height, weight, medications taken, drug sensitivities, allergies, sports, exercise, leisure activities.

Duration of data management:

During the duration of the contract, and after the termination of the agreement, until the end of the limitation period open for asserting a legal claim.

If the data processing defined above requires the presentation of a personal identification document, the Data Controller will accept the personal identification data contained in it without making a copy in view of the public authority of the document, it will not make a photocopy or scan of it, but will certify the presentation of the document and its validity with the signature of the authorized employee.

7) INFORMATION ON THE USE OF COOKIES

Cookies are short data files placed on the user's computer by the visited website. The purpose of cookies is to make the given information communication and Internet service easier and more convenient. There are many types, but they can generally be classified into two large groups:

a temporary cookie that the website places on the user's device only during a specific session (e.g. during the security identification of an Internet banking),

permanent cookie (e.g. language setting of a website), which remains on the computer until the user deletes it.

Based on the guidelines of the European Commission, cookies can only be placed on the user's device with the user's permission, unless they are absolutely necessary for the use of the given service.

In the case of cookies that do not require the user's consent, information must be provided during the first visit to the website. In the case of cookies that require consent, the information can also be linked to the first visit to the website in the event that the data management associated with the use of cookies already begins with the visit to the website.

In accordance with common Internet practice, LifeMax also uses cookies on its website.

During the use of the website, the website of the Data Controller records and manages the following data about the visitor and the device used for browsing:

-the IP address used by the visitor,

-browser type,

-characteristics of the operating system of the device used for browsing (set language)

-date of visit,

-the (sub)page or function visited.

Accepting and authorizing the use of cookies is not mandatory. You can reset your browser settings to reject all cookies or to notify you when a cookie is currently being sent.

However, some website features may not function or function properly without cookies.

The cookies used on the website are not in themselves suitable for identifying the user.

Although most browsers automatically accept cookies by default, they can usually be changed to prevent automatic acceptance and offer a choice each time.

You can find information about the cookie settings of the most popular browsers at the following links:

Google Chrome: https://support.google.com/accounts/answer/61416?hl=hu

Firefox: https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn

Microsoft Internet Explorer 11: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-11

Microsoft Internet Explorer 10: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-10-win-7

Microsoft Internet Explorer 9: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-9

Microsoft Internet Explorer 8: http://windows.microsoft.com/hu-hu/internet-explorer/delete-manage-cookies#ie=ie-8

Microsoft Edge: http://windows.microsoft.com/hu-hu/windows-10/edge-privacy-faq

Safari: https://support.apple.com/hu-hu/HT201265

Cookies used on the website of the Data Controller:

Technically essential session cookies:

These cookies are necessary so that visitors can browse the website and use its functions smoothly and fully. The duration of the data management of these cookies applies only to the visitor's current visit, this type of cookie is automatically deleted from the computer when the session ends or when the browser is closed.

The legal basis for this data management is Act CVIII of 2001 on certain issues of electronic commercial services and information society services. Act (Elkertv.) 13/A. (3) of §

The purpose of data management is to ensure the proper functioning of the website.

Cookies requiring consent:

These enable LifeMax to remember the user's website choices. The visitor can prohibit this data management at any time before using the service and during the use of the service. These data cannot be linked to the user's identification data and cannot be transferred to third parties without the user's consent.

Cookies facilitating use:

The legal basis for data management is the visitor's consent.

Purpose of data management: To increase the user experience, to make the use of the website more convenient. Duration of data management: 6 months.

Performance cookies:

Google Analytics cookies - you can find information about this here:

https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage

Google AdWords cookies - you can find information about this here:

https://support.google.com/adwords/answer/2407785?hl=en

8) OTHER DATA MANAGEMENT

We provide detailed information to the data subject, the data subject's relative, or legal representative about data processing not listed in this Notice when the data is collected.

The court, the prosecutor's office, the investigative authority, the violation authority, the public administrative authority, the National Data Protection and Freedom of Information Authority, or other bodies based on the authorization of the law, may contact the Data Controller in order to provide information, communicate and transfer data, or make documents available. If the authority has indicated the exact purpose and scope of the data, the Data Controller will release personal data to the above authorities only to the extent and to the extent that is absolutely necessary to achieve the purpose of the request.

9) AUTOMATED INDIVIDUAL DECISION MAKING

A decision based on the assessment of the personal characteristics of the data subject may only be made by automated data processing if the decision is:

brought during the conclusion or performance of a contract, provided that it was initiated by the person concerned, or

it is made possible by a law that also establishes measures to ensure the legitimate interests of the data subject.

At the request of the data subject, the Data Controller provides information on the method used during the decision made by automated data processing and its essence. The data subject is entitled to express his point of view.

The Data Controller does not use automated individual decisions during its activities.

10) DATA SECURITY

The Data Controller ensures the confidentiality and security of the handled personal data. To this end, it takes the necessary technical and organizational measures both with regard to data files stored via

IT devices and on traditional, paper-based data carriers. The Data Controller ensures that the data security rules prescribed in the relevant legislation apply.

The Data Manager protects the data with appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage, as well as against becoming inaccessible due to changes in the technology used. In order to enforce the conditions of data security, the Data Controller ensures the appropriate training of the employees concerned.

In order to protect paper-based records, the Data Controller takes the necessary measures, especially in terms of physical security and fire protection.

The employees and other persons acting on behalf of the Data Controller are obliged to securely store and protect the data carriers they use or own that contain personal data, regardless of the method of recording the data, against unauthorized access, alteration, transmission, disclosure, deletion or destruction and against accidental destruction and damage.

In relation to the data of natural persons, the rules on the protection of personal data also apply. The confidentiality obligation - without time limitation - applies to the Data Controller's representative, senior employees, all employees, as well as to all those who have access to information about the data subjects in any way during their activities related to the Data Controller

11) RIGHTS OF INTERESTED PARTIES

11.1. Right to advance information

The data subject has the right to find out about the facts related to the processing of his/her personal data before the data processing begins. The information provided by the Data Controller may also be provided by the Data Controller publishing information on the details of data management locally in the usual manner and drawing the attention of the data subject to this, or even by placing signs to draw the attention of the data subjects prior to the start of data processing (for example, at the entrance of offices, at the beginning of a telephone conversation, in an electronic message, etc.).

The Data Controller strives to ensure that the data subjects receive information about the details of the data management prior to the data management. To this end, the Data Controller publishes information about its data management on its website.

At the request of the data subject, the Data Controller provides information about the data subject's data managed by it or processed by the data processor commissioned by it, its source, the purpose, legal basis, duration of data processing, the name and address of the data processor and its activities related to data processing, the circumstances and effects of any data protection incidents and the measures taken to prevent it, as well as - in the case of forwarding the data subject's personal data - the legal basis and recipient of the data transfer.

The Data Controller is obliged to assess the submitted application as soon as possible - but no later than 25 days - and notify the data subject of the decision in writing, or if the data subject submitted the application electronically, electronically. The information must be provided in an easily accessible and readable form, with concise, clear and clearly worded content.

The Data Controller may refuse to provide information to the data subject only if permitted by law. In this case, the Data Controller informs the data subject about the legal remedies.

11.2. Right of access

At any time, the data subject is entitled to request information about his personal data and information related to their management from the Data Controller.

11.3. Right to rectification

The data subject may request that the Data Controller correct or supplement inaccurate or incomplete personal data. In the event that regular data provision is made based on the data to be corrected, the Data Controller shall, if necessary, inform the recipient of the data provision of the correction or draw the attention of the data subject to the fact that the correction must also be initiated by another data controller.

11.4. Right to erasure and objection

The data subject may request the deletion of his personal data, with the exception of data processing mandated by law. The Data Controller informs the data subject of the deletion. If consent-based data management is a condition for establishing and maintaining the legal relationship of the data subject, the Data Controller will inform the data subject of this and the expected consequences.

The Data Controller refuses to delete personal data if the processing of the data is based on legislation, is linked to the fulfillment of a contractual or legal obligation, or the data processing is necessary to assert the legitimate interests of the Data Controller. In case of refusal to fulfill the deletion request, the Data Controller will inform the data subject of the reason.

The person involved is Isdafoi. you can object to the processing of your personal data in accordance with the provisions of:

if the processing or transmission of personal data is necessary solely for the fulfillment of a legal obligation for the Data Controller or for the enforcement of the legitimate interests of the Data Controller, data receiver or third party, except in the case of mandatory data processing;

if the personal data is used or transmitted for the purpose of direct business acquisition, public opinion polls or scientific research; as well as in other cases specified by law.

11.5. The right to restrict data processing

The data subject is entitled to restrict data processing if:

disputes the accuracy of the processed data,

disputes the legality and/or necessity of data management,

the data subject objected to data processing until the controversial issue is closed.

During the restriction period, the affected data may only be processed with the consent of the affected person, with the exception of storage, or to submit, enforce or defend legal claims, or to protect the rights of other natural or legal persons, as well as for important public interest.

The Data Controller will notify the data subject in advance of the lifting of the restriction.

11.6. Right to data portability

The data subject may request the transfer of all data processed by the Data Controller in relation to him, which the Data Controller has included in its records from the data subject. During the exercise of the right to data portability, the Data Controller transfers the data to the data subject in the form of text, photographs, moving images or audio files on a portable optical data carrier, or in a paper-based document.

11.7. Right to a remedy

The data subjects can directly address their complaints and objections to the Data Controller, who will do his best to eliminate possible legal violations. The Data Controller examines the complaints submitted to it and informs the person concerned of its position and the measures taken.

In the event of information, correction, restriction, deletion, or protest, the Data Controller shall act in accordance with the provisions of the governing legislation. In the event of a violation of rights, the person concerned may request an investigation by the superior manager of the person acting on behalf of the Data Controller, as well as contact the data protection officer of the Data Controller.

In order to investigate the legality of the Data Controller's action, the data subjects may initiate an investigation by the National Data Protection and Freedom of Information Authority:

if the Data Controller limits the enforcement of their rights or rejects their request for the enforcement of these rights, as well as

if, in their opinion, during the processing of their personal data, the Data Controller, or the data processor commissioned or acting on the basis of its instructions, violates the regulations regarding the processing of personal data, defined in law or in a binding legal act of the European Union.

The National Authority for Data Protection and Freedom of Information only investigates complaints if the data subject has already contacted the Data Controller regarding the exercise of the rights indicated in the notification prior to the notification.

Contact information of the National Data Protection and Freedom of Information Authority:

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

Mailing address: 1363 Budapest, Pf. 9.

website: http://www.naih.hu

e-mail: ugyfelszolgalat@naih.hu

Those concerned can assert their claim in court. The lawsuit must be initiated before the competent court at the place of residence or place of residence of the person concerned - at his or her choice.

The Data Controller is responsible for damage caused by illegal data processing in accordance with the provisions of the relevant laws. The Data Controller is obliged to compensate the damage caused by the illegal processing of the data subject's data or by violating the requirements of data security. The Data Controller is also liable to the data subject for the damage caused by the data processor.

The Data Controller is released from liability if it proves that the damage was caused by an unavoidable cause outside the scope of data management. There is no need to compensate the damage if it resulted from the intentional or grossly negligent behavior of the injured party. The Data Controller's general, civil liability under the Civil Code. rules are governing.

At the request of the data subject, the Data Controller provides detailed information on the legal remedies.

12) EXERCISE OF THE RIGHTS OF THE PERSPECTIVES

Those concerned may submit their request for the exercise of their rights orally, in writing or electronically.

By phone (orally): +443300272192

In writing: 4028 Debrecen, Simonyi út 14.

Electronically: contact@lmsoulbuddy.co.uk

The Data Controller fulfills the data subject's request without undue delay, but no later than within 25 days of receipt, in a concise, transparent, comprehensible and easily accessible form, with content that is clearly and comprehensibly formulated. In order to prevent the transmission of data to third parties without authorization, the data manager reserves the right to fulfill the data request only after the data subject has been clearly and unambiguously identified.

The Data Controller also decides on the refusal of the request within this deadline and informs the data subject of the reasons for the refusal of the request, as well as the legal remedies.

The data manager does not charge a fee or reimbursement for the fulfillment of requests. In the event that a new request for the same scope of data is received from the data subject within one year of the previous, already completed request, the Data Controller reserves the right to set a fee for the fulfillment of the request commensurate with the workload related to the fulfillment.

13) FINAL PROVISIONS

This Information Bulletin 21.02.2024. enters into force on

The Data Controller reserves the right to unilaterally amend this Data Management Information. The Notice in force at all times is available on the Data Controller's website (www.lmsoulbuddy.co.uk) and at its headquarters.

Debrecen, 21.02.2024