

PRIVACY POLICY

1. INTRODUCTION

Dorcas Ministries (hereinafter: Data Controller) as a data controller recognizes the content of this legal notice as binding. It undertakes to ensure that all data management related to its activities meets the requirements set out in these regulations and the applicable legislation. The data protection guidelines arising in connection with the data management of the Data Controller are continuously available at <https://www.dorkasz.hu>, or the Data Subject can access them by clicking on the following <https://dorkasz.hu/en/dokumentumok/>.

The Data Controller reserves the right to change this information at any time. Of course, you will notify your audience of any changes in good time. If you have any questions related to this announcement, please write to us and our colleague will answer your question.

The Data Controller is committed to protecting the personal data of its customers and partners, and considers it of utmost importance to respect its customers' right to informational self-determination. The Data Controller treats personal data confidentially and takes all security, technical and organizational measures that guarantee data security. The Data Controller describes its data management practices below:

2. NAME OF DATA PROCESSOR

Name of the donor as operator of the donation platform: Dorcas Ministries
Headquarters (and also the place of complaint handling): 4002 Debrecen, Dorkász tanya 1.
Mailing address: 4002 Debrecen, Erdőspuszta Pf. 146.
Registration number: 09-01-0000048
National ID: 0900/60048/1990/600481990
Tax number: 19122201-1-09
Statistical number: 19122201-9499-569-09
KÖT (public interest voluntary organization) registration number: 8518
Name of registering authority: Debrecen Court
Bank account number: Erste Bank Hungary Zrt., 11993001-02300894
Represented by: Ferenc Vojtkó, chairman of the board of trustees
Electronic correspondence address: alapitvany@dorkasz.hu
Phone number: +36/52/441-119

Data of the hosting provider:

Company name of the hosting provider: DiMa.hu Ltd.

The registered office of the storage service provider is: 44032 Debrecen, Békessy Béla street 9/C. III/10.

Tax number of the storage provider: 14079665-2-09

Registration number of company: 09-09-014017

3. DEFINITION OF THE MORE IMPORTANT TERMS THAT CAN BE FOUND IN THE INFORMATION

- "Respondent": natural persons identified or identifiable on the basis of any information, for whom the Data Controller manages personal data related to them.
- • "Personal data": any information relating to an identified or identifiable natural person ("data subject"); a natural person can be identified directly or indirectly, in particular on the basis of an identifier such as 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.
- • "Data controller": the natural or legal person, public authority, agency or any other body that determines the purposes and means of processing personal data independently or together with others; if the purposes and means of data management are determined by EU or member state law, the data controller or the special aspects regarding the designation of the data controller may also be determined by EU or member state law;
- • "Data management": any operation or set of operations performed on personal data or data files in an automated or non-automated manner, such as collection, recording, organization, segmentation, storage, transformation or change, query, insight, use, communication, transmission, distribution or other by making it available, coordinating or connecting, limiting, deleting or destroying; "Data processor": the natural or legal person, public authority, agency or any other body that processes personal data on behalf 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 protection incident": a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise handled;
- • "Recipient": the natural or legal person, public authority, agency or any other body to whom the personal data is communicated, regardless of whether it is a third party. Public authorities that have access to personal data in accordance with EU or Member State law in the context of an individual investigation are not considered recipients; the handling of said data by these public authorities must comply with the applicable data protection rules in accordance with the purposes of the data management.

4. BASIC PRINCIPLES DURING DATA MANAGEMENT

1. it must be handled lawfully and fairly, as well as in a transparent manner for the data subject ("legality, fair procedure and transparency");
2. should be collected only for specific, clear and legitimate purposes, and should not be handled in a manner incompatible with these purposes; in accordance with Article 89 (1), further data processing for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes is not considered incompatible with the original purpose ("purpose limitation");
3. they must be appropriate and relevant in terms of the purposes of data management, and must be limited to what is necessary ("data economy");
4. they must be accurate and, if necessary, up-to-date; all reasonable measures must be taken to promptly delete or correct personal data that is inaccurate for the purposes of data processing ("accuracy");
5. it must be stored in a form that allows the identification of the subject of whom the data was collected from only for the time necessary to achieve the goals of personal data management; personal data may be stored for a longer period only if the personal data will be

processed in accordance with Article 89 (1) for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, the rights of the subject of whom the data was collected from and subject to the implementation of appropriate technical and organizational measures required to protect your freedoms ("limited storage capacity");

6. must be handled in such a way that adequate security of personal data is ensured through the application of appropriate technical or organizational measures, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage of data ("integrity and confidentiality").

7. The data controller is responsible for compliance with the above principles, and is also able to prove compliance ("accountability").

8. Both when determining the method of data management and during data management, the Data Controller implements appropriate technical and organizational measures - for example pseudonymization - to effectively implement the above principles, fulfill obligations, incorporate legal guarantees, etc. with its purpose, and it does all this in a regulated and detailed manner. In practice, the way of thinking is facilitated by employee education, data protection awareness, and the impact assessment, risk analysis, and interest assessment test ("Privacy by design") used during the introduction and/or regular review of individual data management.

The Data Controller carries out its data management activities based on the following principles for the management of personal data, according to which personal data:

The Data Controller only processes personal data based on the voluntary consent of the affected person, which is necessary for the performance of the service provided to the data subject, defined in the General Terms and Conditions.

During data management, personal data will retain its quality as long as the relationship with the data subject can be restored. The relationship with the data subject can be restored if the Data Controller has the technical conditions necessary for the restoration.

The Data Controller pays special attention to the protection of the personal data of incapacitated persons and minors under the age of 16 with limited legal capacity, children. Their declaration requires the consent of their legal representative, except for those parts of the service where the declaration is aimed at data management that occurs en masse in everyday life and does not require special consideration.

If the personal data was recorded with the consent of the data subject, the Data Controller shall, unless otherwise provided by law, process the recorded data

a) for the purpose of fulfilling the relevant legal obligation, or

b) for the purpose of asserting the legitimate interest of the data controller or a third party, if the assertion of this interest is proportional to the limitation of the right to the protection of personal data without further separate consent, and may be processed even after the consent of the data subject has been revoked.

The Data Controller processes personal data only for specific purposes, in order to exercise rights and fulfill obligations. The Data Controller declares that its data management is everything

meets the purpose, and the data is collected and handled fairly. The Data Controller declares that it only processes personal data that is essential for the realization of the purpose of data management, is suitable for achieving the purpose, and only to the extent and for the time necessary for the realization of the purpose.

The Data Controller declares that it only processes personal data with consent based on adequate information. The Data Controller properly informs the data subject before data processing begins that data processing is based on consent or is mandatory. It informs the data subject - clearly, clearly and in detail - about all the facts related to the processing of their data, in particular the purpose and legal basis of data processing, the person entitled to data processing and data processing, the duration of data processing, if the data controller uses the data subject's personal data with the consent of the data subject and it is handled for the purpose of fulfilling the legal obligation of the data controller or to enforce the legitimate interest of a third party, as well as about who can see the data. The information also covers the data subject's rights and legal remedies.

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

The Data Controller handles personal data legally and fairly, as well as in a transparent manner for the data subject. Infotv. Based on paragraph (2) of § 2, within the framework of the basic principles, Infotv. The Regulation shall be applied in conjunction with the following addition specified in Section 4, Paragraph (5): *"The handling of personal data shall be considered fair and lawful if, in order to ensure the data subject's freedom of expression, the person who wishes to know the data subject's opinion is visited at the data subject's place of residence or residence, provided that, that the data subject's personal data is handled in accordance with the provisions of this law and that the personal inquiry is not for business purposes. Personal inquiries cannot be made on a holiday according to the Labor Code."*

The Data Controller does not check the personal data provided to him. The person providing the data (Data Subject) is solely responsible for the adequacy of the data provided. When any Data Subject provides his/her e-mail address, he/she also assumes responsibility for the fact that only he/she uses the service from the given e-mail address. In view of this assumption of responsibility, any responsibility related to logins made at a specified e-mail address shall be borne solely by the Data Subject who registered the e-mail address.

5. TYPES OF DATA PROCESSING, SCOPE OF PERSONAL DATA, PURPOSE, TITLE AND DURATION OF DATA PROCESSING

The data processing of the Data Controller's activities is based on voluntary consent or the fulfillment of the contract concluded with the data subject. In some cases, however, the management, storage, and transmission of a range of the provided data is made mandatory by law, of which we will notify our audience separately.

We draw the attention of informants to the Data Controller that if they do not provide their own personal data, the informant is obliged to obtain the consent of the data subject.

The data management principles of the Data Controller are in accordance with the applicable legislation related to data protection, in particular the following:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (April 27, 2016) - on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, and on the repeal of Regulation 95/46/EC (general data protection regulation, GDPR);

- CXII of 2011. Act - on the right to self-determination of information and freedom of information (Infotv.),
- CVIII of 2001 Act - on certain issues of electronic commercial services and services related to the information society (Eker.tv.),
- Act C of 2003 - on electronic communications (Eht.),

5.1. DATA PROCESSED DURING WEBSITE USE

You can use the website <https://www.dorkasz.hu> without providing your personal data, accordingly, the use of the website is not covered by the scope of the general data protection regulation.

The Data Controller does not store or manage the data generated during the browsing of the website in any way that can be linked to the specific data subject.

5.2. COOKIE MANAGEMENT OF THE [HTTPS://WWW.DORKASZ.HU](https://www.dorkasz.hu) WEBSITE

The operator of the <https://www.dorkasz.hu> website stores a small data package on the user's computer, so-called places and reads cookies, but does not manage personal data with the help of cookies.

Legal basis for data management: Eker tv. Paragraphs 13.§/A (3), (4), the legal provisions contained in Article 5 (3) of Directive 2002/58/EC, as well as the Ehtv. Based on Section 155 (4), the data subject's consent, which is requested and recorded upon first access to the website.

More information about cookies is available at the following address: <https://dorkasz.hu/en/dokumentumok/>

The user can delete cookies from his computer or disable the use of cookies in his browser. It is usually possible to manage cookies in the Tools/Settings menu of browsers under the Data Protection settings, under the name cookie or cookie.

5.3. DATA MANAGEMENT RELATED TO REGISTRATION AND ACCOUNT CREATION

Type of personal data handled: first name, last name, e-mail address, phone number, city, address, password of the person concerned.

Purpose of data management: By storing the data entered during registration, the Data Controller can provide a more convenient service (e.g. the data subject does not have to be entered again when making a new purchase). Registration is a condition for concluding a contract.

Scope of stakeholders: Every natural person who registers on the website of the Data Controller creates an account.

Legal basis for data management: the consent of the data subject based on Article 6 (1) point a) of the Regulation.

Duration of data management: for the duration of user data storage in the database, until the user's deletion request.

Description of the activity and process involved in data management: In order to place the order, the data subject can register on the website, during which he must provide the information necessary for registration.

Persons entitled to access the data, recipients of the personal data: The Data Controller processes the personal data in order to complete the registration.

5.4. DATA MANAGEMENT RELATED TO ACCESS

Type of personal data handled: e-mail address, password of the person concerned.

Purpose of data management: By storing the data entered during registration and then logging into your own account, the Data Controller can provide a more convenient service (e.g. the data subject does not have to be entered again when making a new purchase). Registration is a condition for concluding a contract.

Scope of those affected: All natural persons who register on the website of the Data Controller and enter their own account.

Legal basis for data management: the consent of the data subject based on Article 6 (1) point a) of the Regulation.

Duration of data management: for the duration of user data storage in the database, until the user's deletion request.

Description of the activity and process involved in data management: In order to place the order, the data subject can register on the website, during which he must provide the information necessary for registration. After that, you can log in to your already created account.

Persons entitled to access the data, recipients of the personal data: The Data Controller processes the personal data in order to complete the registration and login.

5.5. DONATION BY DIRECT BANK TRANSFER

Type of personal data handled: bank transfer data: donor's name, bank account number, name of the account manager's bank, donation amount, transfer date, possibly personal data in the notification

The purpose of the data management is to receive donations by making a transfer to the bank account number 11993001-02300894 maintained by the Data Controller Erste Bank Hungary Zrt.

The scope of those affected: persons making transfers to the Data Controller's own bank account

Legal basis for data management: consent of the data subject based on point a. of Article 6 (1) of the GDPR and on the basis of point c.) of Article 6 (1) of the GDPR § 169 (1) of Act C of 2000 (data management is necessary to fulfill the legal obligation of the data controller)

Duration of data management: from the date of crediting of the transfer to 8 years from the date of acceptance of the accounting report containing the donation in accordance with Section 169 (1) of Act C of 2000; otherwise, until the date of withdrawal of the stakeholder's consent

Data processor: the bank service provider managing the Data Controller's bank account (Erste Bank Hungary Zrt., Headquarters: 1138 Budapest, Népfürdő u. 24-26., Postal address: Erste Bank Hungary Zrt. Budapest 1933, E-mail address: erste@erstebank.hu, Telephone no. : +36 1/298-0222, data protection officer of Erste Bank Hungary Zrt.: Dr. Katalin Fonth, adatvedelem@erstebank.hu)

5.6. DONATION BY BANK CARD PAYMENT (BARION, PAYPAL)

The type of personal data handled: in relation to the form on the Website, in the case of an **individual:** last name, first name, e-mail address, telephone number, address, donation amount, one-time or regular nature of the donation. In the case of a company: company name, tax number, surname, first name, e-mail address, phone number, address, amount of donation, one-time or regular nature of donation

The purpose of the data management: receiving donations in such a way that, after filling out a donor form, the person concerned is redirected to the secure payment

interface operated by Barion or Paypal, on which electronic payment can be made by bank card.

The scope of those affected: persons donating to the beneficiaries by electronic bank card payment

Legal basis for data management: consent of the data subject based on point a. of Article 6 (1) of the GDPR and on the basis of point c.) of Article 6 (1) of the GDPR § 169 (1) of Act C of 2000 (data management is necessary to fulfill the legal obligation of the data controller)

Duration of data management: from the date of crediting of the transfer, according to Section 169 (1) of Act C of 2000, the accounting report containing the donation

for 8 years from the date of its acceptance; otherwise, until the date of withdrawal of the stakeholder's consent

Those entitled to access the data, the recipients of the personal data: We inform those who pay by bank card that the bank card and transaction data are not sent to the Data Controller, the data management related to these data is carried out by Barion and the operator of the Paypal system. The Data Controller only becomes aware of the legal title of the donation ("Accounting with the card acceptor") and the crediting of a cumulative amount during the bank and bookkeeping accounting of the donations. Bank card payments via the Website are always made via the Barion or Paypal payment system. By starting a payment through the Barion or Paypal payment system, the donor acknowledges that the following personal data stored by the Data Controller in the user database of <https://www.dorkasz.hu/> will be transferred to Barion and Paypal as data processors. The range of data transmitted by the data controller is as follows: name, e-mail address, telephone number, billing address data. The nature and purpose of the data processing activity carried out by the data processor can be seen in the Data Management information of Barion or Paypal.

5.7. SUPPORT-RELATED DATA MANAGEMENT

Type of processed personal data: the range of processed data may differ from one support program to another. In the description of the program, the Data Controller always indicates precisely from the list below which personal data of the beneficiaries needs to be provided (personal identification data, health data, data that came to our attention during the assessment of the social situation, data of parents/guardians, photo and audio recordings).

The purpose of Data Management: we process the personal and special data of the beneficiaries and/or their family members in order to be able to select those who can receive the support within the given support program, as well as to ensure that only identifiable and needy persons receive benefits and can receive the program benefits, services, scholarships and other benefits specified in its description.

The scope of those affected: the persons applying for the given support program and/or their family members

Legal basis for data management: GDPR Article 6. (1) point a) the consent of the data subject(s).

Duration of data management: 5 (five) years from the date of the decision in the case of persons applying for the support program but not receiving support, 15 days from the date of receipt of the protest in the case of a protest by the affected party. In the case of supported persons and their family members, until their consent is withdrawn.

5.8. PUBLIC DISCLOSURE OF THE DATA OF SUBSIDIERS AND OTHER PERSONS

Type of processed personal data: the range of processed data is recorded in the agreement between the data subject and the Data Controller, but typically full name, image and/or audio recording of the data subject.

Description of the scope of data management: based on the consent of the grantee or other third party, the full name of the grantee or other third party, the image or voice recording of the grantee, or the personal data of the grantee or other third party on the Website based on the agreement between the data subject and the Data Controller, on our social media platforms and/or publications (Facebook, Instagram).

Purpose of data management: donation to the Data Controller and promotion of the foundation's activities based on the data subject's consent

The scope of those affected: beneficiaries and/or other third parties who have expressly consented in writing to the disclosure of their personal data

Legal basis for data management: GDPR Article 6. (1) point a) of the data subject, as well as the Data Controller's legitimate interest in accordance with Article 6 (1) point f) of the GDPR (an interest assessment test has been prepared, which the data subject can request via the Data Controller's contact details, and the Data Controller makes it available to the data subject issued in the requested form - paper or electronic -).

In order to assert its legitimate interests, the Data Controller may make video and audio recordings for the purpose of documenting its activities for the public benefit and for the purpose of making them known to the public. In view of the fact that - if this is possible - the natural persons visiting the location of the video and audio recordings are informed in advance in writing, or verbally or in the form of short information posted on the site, about the video and audio recordings being made, and we try to make the video and audio recordings in such a way, so that a natural person cannot be directly identified on the basis of them, the data subject's right to self-determination of information and the protection of their privacy are not unreasonably restricted. If the natural person is depicted in the recording in a way that makes

him/her stand out, the legal basis for data processing is in all cases the consent of the relevant GDPR Article 6 (1) point a).

Duration of data management: until the data subject's consent is revoked.

Data processors: (only in case of publication on the given social media platform): See Facebook Ireland Ltd. named in the Data Processors section of this information.

5.9. MANAGEMENT OF DATA OF CORPORATE PARTNERS AND REPRESENTATIVES OF ENTREPRENEURS

Type of personal data handled: personal identification data (first name, last name), contact data (phone number, e-mail address).

The purpose of data management is to maintain contact, and to enforce the legitimate interests of our foundation and the company/enterprise.

Time and method of obtaining the data: at the beginning of the business relationship (when contacting), the personal data of the representatives are recorded in the internal system of our foundation.

Legal basis for data management: The legal basis for processing the above personal data of the contact person of the corporate partner/legal entity entrepreneur is the legitimate interest of our foundation and the corporate partner/legal entity entrepreneur (GDPR Article 6 (1) point f)). It is in the legitimate interest of both parties that business communication takes place effectively during the cooperation and that we are able to provide information to each other's designated representative about any material circumstances affecting the contract concluded between us. The right of informational self-determination of the contact person of the corporate partner/legal person cannot be established, because it is his job duty to facilitate communication between the parties and to provide his personal data for this purpose. The data subject has the right to object to this data processing as described in point 9 of this information.

Duration of data management: until the termination of the contractual relationship with the data subject.

5.10. MANAGEMENT OF DATA OF VOLUNTEER

Type of personal data processed: name, address (place of residence), place and time of birth of the volunteer's mother, e-mail address, telephone number, start date of the volunteer activity, benefits provided to the volunteer, contact details (telephone number, e-mail address) , if the personal data of the volunteers is handled by the Data Controller in the context of casual employment, Act LXXV of 2010 on simplified employment. Act (Efo tv.) § 11, paragraph (1) of the volunteer's name, tax number, tax identification number and social security identification number, during the application

the volunteer can optionally provide additional personal data: when he will be available, what type of work he can do.

Purpose of data management: Recording in a voluntary register, maintaining contact. In the case of volunteers employed as part of casual employment, fulfillment of the statutory reporting obligation.

The time and method of obtaining the data: when submitting the online application as a volunteer, or at the start of casual employment, the personal data of the volunteers are recorded in the internal system of the Data Controller.

Legal basis for data management: Consent of the volunteer (GDPR Article 6 (1) point a)). Consent can be withdrawn at any time. In the case of volunteers acting as casual employees, data management is based on legislation (with regard to point c) of Article 6 (1) of the GDPR, Efo tv. Section 11 (1)).

Duration of data management: 5 years after the end of the voluntary legal relationship (based on § 14 (2) of Act LXXXVIII of 2005).

Those entitled to access the data, the recipients of the personal data: The host organization (Data Manager) may disclose facts, data, and opinions about the volunteer to third parties only in cases specified by law or with the consent of the volunteer. The data relating to the volunteer can be used for statistical purposes and can be transferred for statistical use in a way that is not suitable for personal identification. The data relating to the volunteer to the host organizations for the Central Statistical Office - CLV of 2016 on official statistics. in accordance with § 28 of the Act (hereinafter: Stt.) on the basis of prior verification of the statistical purpose, to the extent necessary for this - in a manner suitable for individual identification for statistical purposes, they must be transferred free of charge and they can be used by the Central Statistical Office for statistical purposes. The range of received data and the detailed rules for data transfer are set out in Stt. must be recorded in the cooperation agreement specified in § 28.

5.11. DATA MANAGEMENT RELATED TO APPLICATION FOR TRAINING

Type of personal data handled: name, e-mail address, telephone number of the applicant for the training, name of the training

The purpose of data management: maintaining contact, completing the training.

Time and method of obtaining the data: when submitting the online application for the training, or at the start of the training, the personal data of the applicants for the training are recorded in the internal system of the Data Controller.

Legal basis for data management: Consent of the data subject (GDPR Article 6 (1) point a). Consent can be withdrawn at any time.

Duration of data management: until the data subject's consent is revoked, failing which, the Civil Code. within the general 5-year statute of limitations.

5.12. DATA MANAGEMENT RELATED TO COMPLAINT HANDLING

Type of personal data handled: Complaint's unique identification number, name, address, telephone number, bank account number (in the case of monetary compensation), place and time of complaint notification, method of complaint notification, related documents (e.g. protocol, notification form), photo.

Purpose of data management: Management, evaluation and registration of quality objections arising in connection with the services offered by the Data Controller.

The scope of the affected parties: In connection with the complaint, we store the data of the customer who submitted the complaint and the administrative staff of the Data Controller.

Legal basis for data management: Administration is started on the basis of consent, the protocol is prepared on the basis of legal obligation. [GDPR Article 6 (1) a) and c)]

Duration of data management: With regard to the records of the complaint and the related documents, the CLV of 1997 on consumer protection. Act 17/A. 5 + 2 years based on § (7).

Description of the activity and process involved in data management: The data management process is carried out in order to issue an invoice in accordance with the law and fulfill the obligation to keep accounting records.

Persons entitled to access the data, recipients of the personal data: The Data Controller handles the personal data related to the complaint in order to fulfill the legal obligation of the minutes taken on the complaint. The consumer protection authority can also be a recipient during a possible investigation.

5.13. DATA MANAGEMENT RELATED TO ASKING A QUESTION AND WRITING FEEDBACK

Type of personal data handled: name, e-mail address, message of the person concerned.

Purpose of data management: The purpose of data management is to provide appropriate information for the data subject and maintain contact.

Scope of stakeholders: All natural persons who contact the Data Controller and request information from the Data Controller in addition to providing their personal data.

Legal basis for data management: the consent of the data subject based on Article 6 (1) point a) of the Regulation.

Duration of data management: for the duration of the provision of the service (until the data is deleted).

Transmission of personal data: During data management, personal data are transmitted to data processors in a contractual relationship with the data controller, for the purpose of performing the services included in the contract, based on the instructions of the Data Controller.

Description of the activity and process involved in data management:

the. The data subject can consult with the Data Controller about the Data Controller's services and/or other related questions, and can also write feedback about the product already received, via the way or method available to him provided by the Data Controller.

b. In accordance with the purpose of data management, the data subject voluntarily consents to the fact that, if he provided his contact information during the information request, the Data Controller will contact him to clarify the question or to answer it for him.

Those entitled to access the data, the recipients of the personal data: The Data Controller, in order to fulfill the answers and maintain contact, and Google Ireland Limited, as a data processor, manage the personal data related to sending messages.

5.14. NEWSLETTER ACTIVITY

The Grt. Pursuant to § 6, the User can give prior and specific consent to be contacted by the Data Controller's newsletters at the contact details provided when registering for the newsletter. Furthermore, with the provisions of this information in mind, the User may consent to the Data Controller handling his personal data necessary for sending advertising offers, as well as to contact him with the Data Controller's advertising offers and other mailings during this data management at the contact details provided during registration.

A cancellation request can be sent to the contact details indicated in the "RIGHTS AND RIGHTS OF THE PERSONS CONCERNED" section of this information, and cancellation can also be requested by clicking on the "Unsubscribe" button at the bottom of the marketing inquiry (newsletter). In case of opt-out, the Data Controller will no longer contact the Data Subject with further newsletters and offers. The Data Subject can unsubscribe from the newsletter free of charge at any time and withdraw their consent to data management.

In this case, the Data Controller will delete all personal data necessary for sending newsletters from its records and will not contact the User with further newsletters.

Type of personal data handled: e-mail address, and the system stores analytical data related to subscription and subscription, sending, delivery and opening of messages, as well as the online activity of the persons concerned (e.g. date and time of events, content viewed, computer IP address, reason for undeliverability).

The purpose of data management: sending electronic messages (e-mail) containing a newsletter to the data subject, providing information about current information, promotions, new functions, current events, programs, providing full, general or personalized information to the recipient about the latest promotions of the Data Controller, about its events, news, notification of changes or non-availability of services.

Stakeholders: All natural persons who wish to be regularly informed about the Data Controller's news, promotions, and discounts, and therefore subscribe to the newsletter service by entering their personal data and clicking on the [I have read and accept the data protection policy] checkbox on the website.

Legal basis for data management: consent of the data subject (GDPR Regulation Article 6 (1) point a) and Grt. Section 6 (5))

Duration of data management: data management lasts until the consent statement is withdrawn, i.e. until unsubscription.

The person of the possible data controllers entitled to access the data, the recipients of the personal data: The personal data can be handled by the Data Controller's customer service staff, in compliance with the above principles, and by Rocket Science Group (Mailchimp) as the data processor.

Possible consequences of failure to provide data: the data subject will not be informed of the data manager's current offers contained in the newsletter.

5.15. DIRECT MARKETING ACTIVITY

Pursuant to point f) of Article 6 (1) of the GDPR Regulation, the Data Controller processes the personal data of donors, volunteers and financial partners based on its legitimate interests, which are necessary for the Data Controller to send them e-mails with direct marketing content exclusively for the purpose of donations content and solely to facilitate donations. Pursuant to this, the Data Controller may contact the Data Subject with electronic mails containing direct marketing, based on this legal basis, the Data Controller shall manage the personal data necessary for sending direct marketing letters, and during this data processing, the Data Controller shall contact the Data Controller with his invitations, offers, and other mailings for the purpose of donations at the contact details previously provided by the Data Subject.

A deletion request can be sent to the contact details indicated in the section "RIGHTS AND RIGHTS OF THE PERSONS CONCERNED" of this information. In the event of a deletion request, the Data Controller will no longer contact the Data Subject with further direct marketing letters and offers. The Data Subject may at any time request the deletion of their personal data regarding direct marketing letters free of charge, in which case the Data Controller will no longer send such letters to the Data Subject. In this case, the Data Controller will also delete all personal data necessary for sending

direct marketing letters from its records and will not contact the User with further direct marketing letters.

Type of personal data handled: e-mail address, and the system stores analytical data related to subscription and subscription, sending, delivery and opening of messages, as well as the online activity of the persons concerned (e.g. date and time of events, content viewed, computer IP address, reason for undeliverability).

Purpose of data management: sending electronic messages (e-mail) containing direct marketing to the data subject, providing information about current information, donations, new functions, current events, programs, providing full, general or personalized information to the recipient about the latest projects of the Data Controller, events, news, notification of changes or non-availability of services.

Scope of those affected: All natural persons who wish to be informed about the Data Controller's news, new projects and discounts, and therefore automatically subscribe to the service of sending direct marketing letters by entering their personal data.

The legal basis for data management: the legitimate interest of the Data Controller (GDPR Regulation Article 6 (1) point f)). Due to the legitimate interest as a legal basis, the Data Controller also carried out an interest assessment test, the result of which is as follows: Based on the interest assessment test, which can be seen by the subject of whom the data was collected from (can be seen at the Data Controller's office or requested from him), it can be established that the legitimate interest of the Data Controller proportionally limits the legitimate interest of the subject of whom the data was collected from. Personal data of the Data Subject

its management is absolutely necessary for the sending of general marketing (advertising) messages, as well as for ensuring the related rights of the subject of whom the data was collected from, and alternative data management solutions involving the management of less personal data or following other methods are not available for its implementation.

Duration of data management: data management lasts until the cancellation request is received, i.e. until you unsubscribe from emails containing direct marketing (advertising), until the cancellation request is evaluated.

The person of the possible data controllers entitled to access the data, the recipients of the personal data: The personal data can be handled by the Data Controller's customer service staff, in compliance with the above principles, and by Rocket Science Group (Mailchimp) as the data processor.

5.16. PRESENCE ON COMMUNITY SITES

The Data Controller is available on various social portals (Facebook, Instagram, Youtube). The Data Controller only communicates with the subject of whom the data was collected from via the social media site, and thus the purpose of the scope of the

processed data becomes relevant when the data subject contacts the Data Controller via the social media site.

The Data Controller operates a Facebook page (Facebook Page) under the address <https://www.facebook.com/DorkaszMinistries/URL> , on which it publishes news, advertisements, displays videos, publishes events, publishes photos, and posts. On the Facebook Page, the Data Controller uses the Facebook Insight (Page Analytics) function to collect, analyze and display data in an aggregated manner on what activities visitors engage in on the page and how much time they spend viewing certain content.

The Data Controller informs the visitors of the Facebook Page that with regard to the personal data collected during Page Analytics related to the Facebook Page, the Data Controller and Facebook Ireland Limited are considered joint (joint) data controllers according to Article 26 of the GDPR, since the data management is jointly determined by Facebook Ireland Limited purposes and means of data management. The agreement on joint data management between the Data Controller and Facebook Ireland Limited regarding the Facebook Page is available here:

https://www.facebook.com/legal/terms/page_controller_addendum

The Data Controller informs the visitors of the Facebook Page about the distribution of the main obligations and responsibilities related to joint data management between the Data Controller and Facebook Ireland Limited, as well as about the essential provisions of the joint data controller agreement:

Facebook Ireland Limited's responsibilities and obligations:

- a) Facebook Ireland Limited assumes primary responsibility for the management of personal data managed in the Page Analytics function; data management is also carried out by Facebook Ireland Limited on behalf of the Data Controller.
- b) Facebook Ireland Limited is responsible for providing the subject of whom the data was collected from with adequate information regarding data management.
- c) Facebook Ireland Limited is responsible for contacting and responding to the subject of whom the data was collected from in the event of the exercise of data subject rights, the Data Controller is not entitled to this based on the joint data management agreement above. If the data subject submits a request regarding the exercise of data subject rights to the Data Controller, the Data Controller must forward it to Facebook Ireland Limited within 7 days, the data subject will receive a response from Facebook Ireland Limited within the statutory deadline.
- d) Facebook Ireland Limited is responsible for complying with data security regulations, reporting data protection incidents and informing the subject of whom the data was collected from about the data protection incident with regard to the data collected and managed during Page Analytics.

Responsibilities and obligations of the Data Controller:

- a) The Data Controller is obliged to ensure that it has a suitable legal basis for data management related to Page Analytics.
- b) The Data Controller is obliged to mark itself as a data controller on the Facebook Page,
- c) The Data Controller may not request from Facebook Ireland Limited the specific personal data handled during Page Analytics, the Data Controller can only see and access the statistics and reports prepared by Facebook Ireland Limited, not the personal data that forms the basis of them.

Type of personal data handled:

- Regarding Facebook Page likes: the number of people liking, the location of the likes, the number of new likes
- In relation to the posts on the Facebook page: how many people the post reached, how many people liked, commented or shared the post, the number of dislikes, the number of hides, the number of reports as spam, the number of people who liked the page when they watch Facebook content
- Regarding visits to the Facebook Page: how many times the page was viewed, how many times they came to the Facebook Page from an external site or website
- Regarding the videos placed on the Facebook Page: how many times the video was viewed for more than 3 seconds, for more than 30 seconds, which are the most viewed videos on the page
- In relation to the visitors of the Facebook Page: for persons liking the Page: gender, age, location (country, city), language; how many people saw the post in the last 28 days, who liked, commented or shared the page in the last 28 days

The purpose of data management: sharing, publishing and marketing the contents of the website on social media. With the help of the social page, the person concerned can also find out about the latest promotions.

Scope of stakeholders: Natural persons who voluntarily follow, share, and like the Data Controller's social media pages or the content appearing on them.

Legal basis for data management: consent of the data subject (GDPR Regulation Article 6 (1) point a) and Grt. Section 6 (5)). Based on the terms and conditions of the social media site, the data subject voluntarily consents to follow and like the content of the Data Controller. Using an exemplary definition, the data subject can subscribe to the news feed published on the message wall on the Facebook page by clicking on the "like" link on the page, and thereby consents to the publication of the Data Controller's news and offers on his own message wall, and the "dislike"/ You can unsubscribe by clicking on the "don't like it" link, and you can delete unwanted news feeds appearing on the message wall using the message wall settings.

With regard to the Data Controller, the legal basis for the data management of the above data is therefore consent according to Article 6, Paragraph 1, Point a) of the GDPR. The data subject can withdraw his consent at any time. It is possible to give or withdraw consent in the Facebook profile of the person concerned. It is the duty of Facebook Ireland

Limited to publish the detailed data management information regarding data management related to the Facebook Page based on the joint data management agreement referred to above.

The Data Controller disclaims responsibility for data processing by Facebook Ireland Limited, Facebook Ireland Limited is solely responsible for that.

Duration of data management: until deletion at the request of the data subject. The data subject can receive information about the data management of the given social media site on the given social media site.

5.17. DATA MANAGEMENT RELATED TO AUTHORIZATION OF CONTRIBUTION

Type of personal data handled: IP address, e-mail address, date of consent

Purpose of data management: During the registration and order, the IT system stores the IT data related to the consent for later provability.

The scope of those affected: All natural persons who register on the Data Controller's website, place an order, or subscribe to a newsletter.

Legal basis for data management: based on legal obligation (based on GDPR Article 6 (1) point c), this obligation is prescribed by Article 7 (1) of the GDPR Regulation.

Duration of data management: Due to legal requirements, the consent must be proven later, therefore the data storage period is stored for a period of limitation after the termination of data management.

5.18. EXTERNAL LINKS AND REFERENCES

Our website may contain many connection points (links, references) that lead to the pages of other service providers, so the website visitor may reach websites whose data is not managed by the Data Controller. The Data Controller assumes no responsibility for the data and information protection practices of these service providers.

These links are:

- <https://creativesales.hu>
- <https://www.youtube.com>
- <https://www.instagram.com>
- <https://www.facebook.com>
- www.coopszolnok.hu
- www.ordogpapier.hu
- <https://www.gsv.hu>
- <https://aveasvanyviz.hu>
- <https://www.toyota.hu>
- www.litografia.hu
- <https://www.szabadosok.hu>

- <https://www.feherdani.com>
- <https://www.baromfiudvar.hu>
- www.karpatokalapitvany.hu

Facebook button

The website may use social plugins of the facebook.com social network operated by Facebook Ireland Ltd. (4 Grand CanalSquare, Grand CanalHarbour, Dublin 2, Ireland) ("Facebook"). The plugins can be recognized by the Facebook logos (white letter "f" on a blue background, "Like", "Like" or thumbs up) and are marked by the term "Facebook Social Plugin". The list and appearance of Facebook's social plugins can be found on the following page:

<https://developers.facebook.com/docs/plugins/>.

If you use a function of this website that includes one of the above plugins, your device establishes a direct connection with Facebook's servers. The content of the plugin is sent directly to your device by Facebook and integrated into our online service from there. Usage profiles can be generated from the processed data. We cannot influence which data Facebook obtains with the help of the plugin, so we inform users based on our knowledge.

By installing the plugin, Facebook is informed that you have opened the relevant website. If you are logged in to Facebook, Facebook can assign the visit to your Facebook account. If you interact with the plugin, i.e. click the "Like" button or comment, the relevant data from your device will be transmitted directly to Facebook and stored there. If you do not have a Facebook account, it is still possible for Facebook to learn and store your IP address.

You can find information about the purpose and scope of the acquisition, further processing and use of data by Facebook, as well as the rights and setting options related to the protection of your privacy in Facebook's data management policy: <https://www.facebook.com/about/privacy/>.

If you are a member of Facebook and do not want Facebook to collect data about you on this website and link it to your profile data stored by Facebook, you must log out of Facebook and delete cookies before using our online service. Additional settings and disabling the use of data for advertising purposes can be specified in the Facebook profile settings:

<https://www.facebook.com/settings?tab=ads>,

US site address: <http://www.aboutads.info/choices/>,

the EU site is <http://www.youronlinechoices.com/>.

The settings are platform-independent, meaning they apply to both desktop and mobile devices.

More information about the privacy policies of Google and Facebook can be found at the following contacts:

<http://www.google.com/privacy.html> and <https://www.facebook.com/about/privacy/>

Instagram button

The functions of the Instagram service are embedded on the website. These integrated features are provided by Instagram Inc. (1601 Willow Road, Menlo Park, CA, 94025, USA). If you are logged in to your Instagram account, you can link the content of our website to your Instagram profile by clicking the Instagram button. This allows Instagram to assign your visit to our website to your user account. We would like to inform you that, as the provider of the website, we have no knowledge of the content of the transmitted data and its use by Instagram.

You can find information about the information collected by Instagram and its use in the data protection policy at the following address:

<http://instagram.com/about/legal/privacy/>.

YouTube button

We use the youtube.com YouTube button plugin operated by YouTube LLC (901 Cherry Ave, San Bruno, CA 94066, USA), a subsidiary of Google Inc. (1600 Amphitheater Parkway, Mountain View, CA 94043, USA). The plugin can be recognized by the YouTube logo. When you visit a page of the website that has a YouTube plugin, a connection is established with the YouTube servers. This informs the YouTube server which website was visited. If you have a YouTube account and are logged in, YouTube can directly assign your browsing behavior to your personal profile. If you log out of your YouTube account, you can prevent this assignment. You can find more information about the collection and use of data collected by YouTube at the following address:

https://www.youtube.com/static?template=privacy_guidelines.

Embedded YouTube videos

We embed YouTube videos. Embedded videos place cookies on the user's computer when the website is opened. If you have deactivated the storage of cookies in Google's advertising program, you cannot expect such cookies when you open YouTube clips either. At the same time, YouTube also stores usage data independent of the user in other cookies. If you wish to prevent this, you must set the appropriate settings in your browser.

In order to make a decision, the Data Controller does not apply purely automated data management or individual measures for the purpose of profiling in accordance with Article 4, point 4 of the GDPR.

5.20. OTHER DATA MANAGEMENT

We provide information on data management not listed in this data management information when the data is collected. We inform our customers that the court, the prosecutor, the investigative authority, the infringement 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 manager. If the authority has specified the exact purpose and scope of the data, the Data Controller will only release personal data to the authorities to the extent and to the extent that is absolutely necessary to achieve the purpose of the request.

6. CLAIMS OF DATA PROCESSOR(S).

The Data Controller uses data processors in order to facilitate its own data management activities, as well as in order to fulfill its contractual obligations with the data subject and the obligations imposed by legislation, which means that we transfer your personal data, also recorded in this data protection information, to the data processor concerned with the given service.

The Data Controller places great emphasis on using only those data processors who provide adequate guarantees for the implementation of appropriate technical and organizational measures ensuring compliance with the requirements of the GDPR and the protection of the rights of the subject of whom the data was collected from

The data processor and any person acting under the control of the data processor and having access to personal data handle the personal data contained in this information only in accordance with the instructions of the data controller.

The Data Controller is legally responsible for the activities of the data processor. The data processor is only liable for damages caused by data processing if it has not complied with the obligations specifically imposed on data processors specified in the GDPR, or if it has ignored or acted contrary to the lawful instructions of the Data Controller.

The data processor has no meaningful decision-making regarding the management of the data. The data processors keep the data for the same period as the Data Controller, after which they are deleted. The Data Controller is entitled to check compliance with data protection and security requirements.

The data manager uses the following data processors.

	Data processor
Name:	DiMa.hu Ltd.
Headquarters:	4032 Debrecen, Békessy Béla street 9/C. III/10.

Tax number:	14079665-2-09
Registration number:	09-09-014017
Name of the data processing activity:	hosting service
	Data processor
Name:	Google Ireland Limited
Registered office:	Gordon House, Barrow Street, Dublin 4, Ireland
Registration number:	368047
Court of record:	Operates under the laws of Ireland
Website:	www.google.com
Name of the data processing activity:	mail system management
	Data processor
Name:	The Rocket Science Group, LLC (Mailchimp)
Headquarters:	675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA
Website:	https://mailchimp.com
Name of the data processing activity:	newsletter database management

The Data Controller reserves the right to use an additional data processor, the identity of which will be provided individually at the latest at the start of data processing.

7. DATA TRANSFER TO THIRD PARTIES

"third party": the natural or legal person, public authority, agency or any other body that is not the same as the data subject, your data manager, the data processor or the persons who have been authorized to process personal data under the direct control of your data manager or data processor.

	Third-party (independent) data controller
Neve:	PayPal (Europe) S.à.r.l. et Cie, S.C.A.
Registered office:	LegalDepartment, 22-24 Boulevard Royal, 2449 Luxembourg, Luxembourg
Company registration number:	R.C.S. Luxembourg B 118 349
E-mail:	enquiry@paypal.com
Website:	https://www.paypal.com
Name of the activity:	online payment service provider
	Third-party (independent) data controller
Name:	Barion Payment Zrt.
Headquarters:	1117 Budapest, Irinyi József u. 4-20. 2. emelet
E-mail:	compliance@barion.com
Phone:	+36-1-464-7099
Website:	https://barion.com
Name of the activity:	electronic money institution
	Third-party (independent) data controller
Name:	ERSTE BANK HUNGARY Limited Liability Company
Headquarters:	1138 Budapest, Népfürdő street 24-26.
Tax number:	10197879-4-44

Company registration number	Cg. 01-10-041054
Registering court:	Company Court of the Capital City Court
Represented by:	Jelasity Radován, CEO
E-mail:	erste@erstebank.hu
Phone:	+36-1-298-0222
Website:	https://www.erstebank.hu
Name of the activity:	payment service provider
	Third-party (independent) data controller
Name:	PayPal (Europe) S.à.r.l. et Cie, S.C.A.
Registered office:	LegalDepartment, 22-24 Boulevard Royal, 2449 Luxembourg, Luxembourg
Website:	https://www.paypal.com
Name of the activity:	online payment (paypal)
	Third-party (independent) data controller
Name:	Facebook Ireland Ltd. (Facebook és Instagram)
Registered Office:	4 Grand CanalSquare Grand CanalHarbour Dublin 2 Ireland
Name of the activity:	Delivery of specific, targeted electronic advertisements to the Data Subject based on personal data approved by the Data Subject for the purpose of advertising.
	Third-party (independent) data controller
Name:	YouTube LLC.
Registered Office:	901 Cherry Ave., San Bruno, CA 94066, United States
Name of the activity:	video sharing

In addition to the above, the Data Controller may forward the processed personal data to additional recipients if this is necessary to fulfill contractual or statutory obligations. These may be: organizations issuing tenders, public bodies, authorities, courts, prosecutor

8. DATA STORAGE

The data controller stores the personal data of the data subject on the server operated by Júlia Gyarmati Csilla ev.

9. DATA SECURITY MEASURES

The Data Controller stores data in electronic form on the server and computers located at the headquarters, and paper-based data in archives at its headquarters, locations and warehouses. Paper-based data is stored in lockers/rooms that can be locked.

The Data Controller and its data processors implement appropriate technical and organizational measures, taking into account the state of technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of data management, as well as the varying probability and severity of the risk to the rights and freedoms of natural persons, in order to ensure that a level of data security corresponding to the degree of risk is guaranteed.

The Data Controller selects and operates the IT tools used to manage personal data in such a way that the managed data:

- accessible to those authorized to do so (availability);
- its authenticity and authentication are ensured (authenticity of data management);
- its immutability can be verified (data integrity);
- be protected against unauthorized access (data confidentiality).

The Data Manager protects the data with appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction, damage, and inaccessibility resulting from changes in the technology used.

In order to protect the data files managed electronically in its various records, the Data Controller ensures with an appropriate technical solution that the stored data cannot be directly linked and assigned to the data subject, unless permitted by law.

In view of the current state of technology, the Data Controller ensures the protection of the security of data management with technical, organizational and organizational measures that provide a level of protection corresponding to the risks associated with data management.

The Data Controller keeps it during data management

- confidentiality: protects the information so that only those who are authorized to do so can access it;
- integrity: protects the accuracy and completeness of the information and the method of processing;
- availability: it ensures that when the authorized user needs it, he can really access the desired information and that the related tools are available.

The IT system and network of the Data Controller and its partners involved in data management are both protected against computer-supported fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, computer intrusions and denial-of-service attacks. The operator ensures security with server-level and application-level protection procedures. We inform users that electronic messages transmitted on the Internet, regardless of the protocol (e-mail, web, ftp, etc.), are vulnerable to network threats that lead to unfair activity, contract disputes, or the disclosure or modification of information. To protect against such threats, the Data Controller takes all the necessary precautions. Monitors systems to capture any security discrepancies and provide evidence for any security incidents. In addition, system monitoring also makes it possible to check the effectiveness of the precautions used.

The Data Controller keeps records of any data protection incidents, indicating the facts related to the data protection incident, its effects and the measures taken to remedy it. The Data Controller shall report any data protection incident to the National Data Protection and Freedom of Information Authority without delay and, if possible, no later than 72 hours after becoming aware of the data protection incident, unless the data protection incident is likely to pose no risk to the rights and freedoms of natural persons looking at. If the notification is not made within 72 hours, the reasons justifying the delay must also be attached.

The Data Controller does not transfer personal data outside the territory of the European Economic Area.

10. THE RIGHTS AND OPTIONS OF RIGHTS ENFORCEMENT OF THE PERSONS INVOLVED

The data subject can request information about the processing of his personal data, and can request the correction of his personal data, or - with the exception of mandatory data processing - deletion or withdrawal, he can exercise his right to data portability and protest as indicated when the data was collected, or at the above contact details of the Data Controller.

10.1. Right to information

The Data Controller takes appropriate measures in order to provide the subject of whom the data was collected from with all information regarding the processing of personal data referred to in Articles 13 and 14 of the GDPR and Articles 15-22. and provide each piece of information according to Article 34 in a concise, transparent, comprehensible and easily accessible form, clearly and comprehensibly worded.

10.2. The data subject's right of access

The data subject is entitled to receive feedback from the Data Controller as to whether his personal data is being processed, and if such data processing is underway, he is entitled to access the personal data and the following information:

- the purposes of data management;
- categories of personal data concerned;
- the recipients or categories of recipients to whom or to whom the personal data has been or will be communicated, including in particular recipients in third countries and international organizations;
- the planned period of storage of personal data;
- the right to correct, delete or limit data processing and to protest;
- the right to submit a complaint to the supervisory authority;
- information about data sources;
- the fact of automated decision-making, including profiling, as well as comprehensible information about the applied logic and the significance of such data management and the expected consequences for the data subject.

The Data Controller shall provide the information within a maximum of one month from the date of submission of the request.

10.3. Right to rectification

The data subject may request the correction of inaccurate personal data concerning him or her managed by the Data Controller and the addition of incomplete data.

10.4. Right to erasure

If one of the following reasons exists, the data subject has the right to request that the Data Controller delete his/her personal data without undue delay:

- the personal data are no longer needed for the purpose for which they were collected or otherwise processed;
- the data subject withdraws the consent that forms the basis of the data management, and there is no other legal basis for the data management;
- the data subject objects to the data processing and there is no overriding legal reason for the data processing;
- personal data were handled illegally;
- personal data must be deleted in order to fulfill the legal obligation prescribed by EU or Member State law applicable to the data controller;
- the collection of personal data took place in connection with the offering of services related to the information society.

Data deletion cannot be initiated if data management is necessary:

- for the purpose of exercising the right to freedom of expression and information;
- for the purpose of fulfilling the obligation under the EU or Member State law applicable to the data controller, requiring the processing of personal data, or for the execution of a task carried out in the public interest or in the context of the exercise of public authority granted to the data controller;
- relating to the field of public health, or for archival, scientific and historical research purposes or for statistical purposes, based on public interest;
- or to submit, assert or defend legal claims.

10.5. The right to restrict data processing

At the request of the data subject, the Data Controller restricts data processing if one of the following conditions is met:

- the data subject disputes the accuracy of the personal data, in this case the limitation applies to the period that allows checking the accuracy of the personal data;
- the data management is illegal and the data subject opposes the deletion of the data and instead requests the restriction of their use;
- the data controller no longer needs the personal data for the purpose of data management, but the data subject requires them to submit, enforce or defend legal claims; obsession
- the data subject objected to data processing; in this case, the restriction applies to the period until it is determined whether the legitimate reasons of the data controller take precedence over the legitimate reasons of the data subject.

If data management is subject to restrictions, personal data may only be processed with the consent of the data subject, with the exception of storage, or to submit, enforce or defend legal claims, or to protect the rights of another natural or legal person, or in the important public interest of the Union or a member state.

10.6. Right to data portability

The data subject has the right to receive the personal data concerning him/her provided to the Data Controller in a segmented, widely used, machine-readable format, and to forward this data to another data controller.

10.7. Right to protest

The data subject has the right to object at any time, for reasons related to his own situation, to the processing of his personal data necessary for the performance of a task carried out in the public interest or within the framework of the exercise of public authority conferred on the Data Controller, or for the enforcement of the legitimate interests of the data controller or a third party, including profiling based on the aforementioned provisions too. In the event of a protest, the Data Controller may no longer process the personal data, unless it is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or that are related to the submission, enforcement or defense of legal claims.

10.8. Automated decision-making in individual cases, including profiling

The data subject has the right not to be covered by the scope of a decision based solely on automated data management, including profiling, which would have a legal effect on him or affect him to a similar extent. The Data Controller does not perform automated decision-making based on automated data management or profiling.

10.9. Right of withdrawal

The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the legality of data processing based on consent prior to withdrawal. Before giving consent, the data subject must be informed of this. It should be possible to withdraw consent in the same way as to give it.

10.10. Right to go to court

In the event of a violation of their rights, the data subject may go to court against the Data Controller, i.e. file a lawsuit at the competent court of their place of residence (place of stay) (you can view the list of courts by clicking on the following link: <http://birosag.hu/torvenyszek>). The court acts out of sequence in the case.

10.11. Data protection official procedure

You can file a complaint with the National Data Protection and Freedom of Information Authority:

Name: National Data Protection and Freedom of Information Authority

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

Mailing address: 1363 Budapest, Pf.: 9.

Phone: 0613911400

Fax: 0613911410

E-mail: ugyfelszolgalat@naih.hu

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

10.12. Informing the data subject about the data protection incident

If the data protection incident is likely to involve a high risk for the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the data protection incident without undue delay.

In the information provided to the data subject, the nature of the data protection incident must be clearly and comprehensibly described, and the name and contact information of the data protection officer or other contact person providing additional information must be provided; the likely consequences of the data protection incident must be described; the measures taken or planned by the Data Controller to remedy the data protection incident must be described, including, where applicable, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

The data subject does not need to be informed if any of the following conditions are met:

- the Data Controller has implemented appropriate technical and organizational protection measures and these measures have been applied to the data affected by the data protection incident, in particular those measures - such as the use of encryption - that make them unintelligible to persons not authorized to access personal data the data;
- after the data protection incident, the Data Controller took additional measures to ensure that the high risk to the rights and freedoms of the data subject is unlikely to materialize in the future;
- providing information would require a disproportionate effort. In such cases, the subject of whom the data was collected from must be informed through publicly published information, or a similar measure must be taken that ensures similarly effective information to the subject of whom the data was collected from.

If the Data Controller has not yet notified the data subject of the data protection incident, the supervisory authority, after considering whether the data protection incident is likely to involve a high risk, may order the data subject to be informed.

10.13. Compensation and damages

Any person who has suffered material or non-material damage as a result of a violation of the data protection regulation is entitled to compensation from the Data Controller or the data processor for the damage suffered. The data processor is only liable for damages caused by data processing if it has not complied with the obligations specified in the law, which are specifically imposed on data processors, or if it has ignored or acted contrary to the lawful instructions of the Data Controller.

If several data managers or data processors or both data managers and data processors are involved in the same data management and are liable for damages caused by data management, each data manager or data processor is jointly and severally liable for the entire damage.

The Data Controller or the data processor is exempted from liability if it proves that it is not in any way responsible for the event causing the damage.

10.14. Procedural rules

- The Data Controller informs the data subject without undue delay, but in any case within one month of receipt of the request, in accordance with Articles 15-22 of the GDPR, on measures taken following a request pursuant to Art.
- If necessary, taking into account the complexity of the application and the number of applications, this deadline can be extended by another two months. The Data Controller shall inform the data subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request. If the data subject submitted the request electronically, the information will be provided electronically, unless the data subject requests otherwise.
- If the Data Controller does not take measures following the data subject's request, it shall inform the data subject without delay, but at the latest within one month of the receipt of the request, of the reasons for the failure to take action, as well as of the fact that the data subject may file a complaint with a supervisory authority and exercise his right to judicial redress .
- The Data Controller provides the requested information and information free of charge. If the data subject's request is clearly unfounded or - especially due to its repeated nature - excessive, the data controller may, taking into account the administrative costs associated with providing the requested information or information or taking the requested measure, charge a reasonable fee or refuse to take action based on the request.
- The Data Controller informs all recipients of all corrections, deletions or data management restrictions carried out by him or her, with whom the personal
- data, unless this proves to be impossible or requires a disproportionately large effort. At the request of the data subject, the Data Controller informs about these recipients.
- The Data Controller provides a copy of the personal data that is the subject of data management to the data subject. For additional copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs. If the data subject submitted the request electronically, the information will be provided in electronic format, unless the data subject requests otherwise.

11. REVIEW IN CASE OF MANDATORY DATA MANAGEMENT

If the duration of mandatory data processing or the periodic review of its necessity is not determined by law, local government decree or a mandatory legal act of the European Union, the data controller shall review at least every three years from the start of data processing that

the processing of personal data handled by him or by the data processor acting on his behalf or at his direction is in order to achieve the purpose of data processing is it necessary.

The data controller documents the circumstances and results of this review, keeps this documentation for ten years after the completion of the review and makes it available to the Authority at the request of the National Data Protection and Freedom of Information Authority (hereinafter: the Authority).

12. MODIFICATION OF DATA MANAGEMENT INFORMATION

The Data Controller reserves the right to modify this data management information in a way that does not affect the purpose and legal basis of data management. By using the website after the amendment enters into force, you accept the amended data management information.

If the Data Controller wishes to carry out further data processing in relation to the collected data for a purpose other than the purpose of their collection, it will inform you of the purpose of the data processing and the following information before the further data processing:

- the period of storage of personal data, or if this is not possible, the aspects of determining the period;
- your right to request from the Data Controller access to your personal data, their correction, deletion or restriction of processing, and in the case of data processing based on legitimate interests, you may object to the processing of personal data, and in the case of data processing based on consent or a contractual relationship, you may request data portability securing the right;
- in the case of consent-based data management, that you can withdraw your consent at any time,
- on the right to submit a complaint to the supervisory authority;
- whether the provision of personal data is based on a legal or contractual obligation or is a prerequisite for entering into a contract, as well as whether you are obliged to provide personal data, and what possible consequences the failure to provide data may have;
- the fact of automated decision-making (if such a procedure is used), including profiling, as well as, at least in these cases, comprehensible information about the logic used and the significance of such data management and the expected consequences for you.

The data processing can only start after this, if the legal basis of the data processing is consent, in addition to the information, you must also consent to the data processing.