

PRIVACY NOTICE

This Privacy Notice is effective as of 2022.01.24

FTC Kereskedelmi Kft. makes utmost efforts to process, store and use personal data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter the 'Regulation').

In connection with the processing of the data, FTC Kereskedelmi Kft. hereby informs users of the website www.shop.fradi.hu (hereinafter: the Website) and data subjects placing an order (hereinafter: the 'Data Subject') about the personal data processed by it, and the principles and practices it applies during personal data processing.

Personal data collected by the Controller may be processed only for clearly determined and legitimate purposes and may not be processed for any other purpose, and shall be stored so that it enables the identification of Data Subjects only for the time required for achieving the purposes of data processing.

The Controller shall ensure that no unauthorised person may inspect the personal data and that the personal data shall be stored so as to make sure that it cannot be accessed, viewed, modified or destroyed by any unauthorised person.

1. DATA CONTROLLER'S DETAILS

Name:	FTC Kereskedelmi Kft.
Seat, operating site, mail address:	1091 Budapest, Üllői út 129.
Company registration number:	01-09185023
VAT number:	24836333-2-43
Registering authority:	Court of Registration of the Budapest Metropolitan Court
E-mail address:	adatvedelem@fradi.hu

2. DATA PROCESSING CASES

2.1. Registration

Data being processed: surname, given name, email address, password. After registration, the following additional data is required for performing the order: delivery address and billing address: postal code, city, street, house number, telephone number and, in the case of companies, tax number.

The purpose of data processing: To enable shopping on the website as a registered user, thus providing convenience features ensuring that it is not necessary to re-enter the data required to perform subsequent orders.

Duration of data processing: the processing of personal data that must be provided during registration starts with the registration and lasts until it is deleted upon request. If the Data Subject does not request the cancellation of their registration, the Controller shall delete it from its system no later than 30 days after the termination of the Website.

Legal basis for data processing: If the Data Subject purchases without registration, the legal basis is the Data Subject's voluntary consent pursuant to Article 6(1)(a) of the Regulation. If the Data Subject wishes to use a fan card for the order, the purchase is binding and its legal basis is legitimate interest pursuant to Article 6(1)(f) of the Regulation.

Source of data: collected directly from the Data Subject.

The e-mail address does not need to contain personal data, e.g. the e-mail address does not need to contain the Data Subject's name. The Data Subject is free to decide whether they provide an existing e-mail address that contains information indicating their identity.

Cancelling registration: the registration can be cancelled with a cancellation request sent to the Controller. Upon receipt of the cancellation request, the Controller shall immediately delete the Data Subject's user account together with all personal data. However, the cancellation does not imply destruction of invoices related to orders already placed, or the deletion of data that is necessary to fulfil the Controller's legal obligations (e.g. to retain a complaint for 3 years). After deletion, the data can no more be restored.

Categories of recipients of personal data: database management partner, invoicing, order processing

The consequence of the absence of data processing: the Data Subject will be unable to use the convenience functions associated with registration, and will not be authorised to create or use a user account.

2.2. Login/registration with Facebook account

If the Data Subject has a Facebook account, they can register by clicking the "Register with Facebook" button, or log in to the Website by clicking the "Log in with Facebook" button. In this case, the Data Subject will be redirected to the external service provider's login request page, where they can log in to the Data Controller's website with the previously provided (on the Facebook page) registered data. The Data Controller does not have access to or store the entered password data. Registration is not mandatory in this case either.

Scope of processed data: name, email address, Facebook ID

Purpose of data processing: identification of the Data Subject and ensuring that the Data Subject can easily register/log in to the Website registration interface with the data of their existing Facebook account.

Legal basis for data processing: Voluntary consent of the Data Subject pursuant to Article 6(1)(a) of the Regulation.

Duration of data processing: the processing of personal data required during registration begins with registration and lasts until its deletion upon request. If the Data Subject does not request the deletion of their registration, the Data Controller will delete the Data Subject's personal data from its system no later than 30 days after the termination of the Website.

Source of data: collected directly from the Data Subject.

Consequence of failure to process data: no adverse legal consequences.

2.3. Login/registration with a Google account

If the User has a Google account, they can log in by clicking the "Login with Google" button or register by clicking the "Register with Google" button in order to make purchases or use services on the Website. Registration is not mandatory in this case either.

Scope of processed data: name, email address, Google ID

The data subject will be redirected to the external service provider's login page, where he/she can log in to the Data Controller's website with the previously provided (on the Google website) registered data. The Data Controller does not have access to or store the entered password data.

Purpose of data processing: Identification of the Data Subject, ensuring that the Data Subject can easily register/log in to the registration/log in interface of the Website using the data of his/her existing Google account.

Legal basis for data processing: Voluntary consent of the Data Subject pursuant to Article 6(1)(a) of the Regulation.

Duration of data processing: the processing of personal data mandatorily provided during registration begins with the registration and lasts until its deletion upon request. If the User does not request the deletion of his/her registration, the Data Controller will delete the User's personal data from its system no later than 30 days after the termination of the Website.

Data source: collected directly from the Data Subject.

Consequence of failure to process data: no adverse legal consequences.

2.4. Placing an order with registration

Data being processed: surname, given name, e-mail address, telephone number, billing and shipping details such as postcode, city, street name, house number, floor, door no., tax number for companies, fan card number (optional) user identification fan discount card ID (optional).

The purpose of data processing: to conclude a contract, perform an order, modify or complete the order if necessary, liaise in relation to the performance of the order, provide home delivery of the product.

Legal basis for data processing: performance of a contract pursuant to Article 6(1)(b) of the Regulation or a legitimate interest pursuant to Article 6(1)(f) of the Regulation for 5 years after the performance of the order.

Controller's legitimate interest (if the legal basis is legitimate interest): in the case of the second legal basis above, to ensure provability in case of legal disputes and authority enquiries.

Duration of data processing: for 5 years after the performance of the contract.

Source of data: collected directly from the Data Subject.

Categories of recipients of personal data: logistics partner, database management partner, order processing

The consequence of the absence of data processing: the Data Subject will be unable to complete the ordering process.

2.5. Buying without registration

Data being processed: surname, given name, e-mail address, telephone number, billing and shipping details such as postcode, city, street name, house number, floor, door no., tax number for companies.

The purpose of data processing: to conclude a contract, perform an order, modify or complete the order if necessary, liaise in relation to the performance of the order, provide home delivery of the product.

Legal basis for data processing: performance of a contract pursuant to Article 6(1)(b) of the Regulation or a legitimate interest pursuant to Article 6(1)(f) of the Regulation for 5 years after the performance of the order.

Controller's legitimate interests (if the legal basis is legitimate interest): in the case of the second legal basis above, to ensure provability in case of legal disputes and authority enquiries.

Duration of data processing: Personal data may be deleted at any time after the request for deletion has been sent. Upon receipt of the request, the Controller will delete the personal data from its system within 5 working days.

Categories of recipients of personal data: logistics partner, database management partner, order processing

The consequence of the absence of data processing: the Data Subject will be unable to complete the ordering process.

2.6. Issuing the invoice for the order

Data being processed: surname, given name, home address (mandatory).

The purpose of data processing: to perform the invoicing obligation and comply with accounting principles, prepare and record accounts.

Legal basis for data processing: compliance with a legal obligation pursuant to Article 6(1)(c) of the Regulation. (VAT Act/Act CXXVII of 2007 on Value Added Tax)

Duration of data processing: the invoice will be kept for 8 years.

Categories of recipients of personal data: tax authority, and other authorities, courts if necessary and upon request.

Source of data: collected directly from the Data Subject.

The consequence of the absence of data processing: the Controller will be unable to perform its legal obligations specified in the applicable Hungarian laws.

No data transfer takes place outside the EU.

2.7. Customer correspondence, liaising, establishing contact

Data being processed: depending on the contact platform: surname, given name, e-mail address, telephone number, other (optional) data provided by the Data Subject.

The purpose of data processing: if the Data Subject has a question related to the Website or the Controller's service, they may contact the Controller via the contact form or the other contact details provided in this Notice and on the interface of the Website. It enables establishing contact and liaising between the Controller and the Data Subject in connection with the issue.

Duration of data processing: The Controller handles the e-mails and postal letters received by it, together with the sender's name, e-mail address and other personal data provided in the message, from the time of data disclosure until the Data Subject's question or comments have been resolved or answered.

Legal basis for data processing: the Data Subject's voluntary consent pursuant to Article 6(1)(a) of the Regulation.

Categories of recipients of personal data: database management partner, customer relationship administration

Source of data: collected directly from the Data Subject.

Possible consequences of refusing data disclosure: the customer cannot be contacted by mail.

No data transfer takes place outside the EU.

2.8. Complaint handling

Data being processed: depending on the contact platform: surname, given name, e-mail address, telephone number, complaint submitted by the Data Subject.

The purpose of data processing: if the Controller handles the Data Subject's complaint in connection with the provided service, it also processes personal data during the process. The purpose of data processing is to implement complaint handling in accordance with applicable laws, as well as to establish and keep contact between the Controller and the Data Subject in connection with the complaint.

Duration of data processing: Pursuant to Act CLV of 1997 on Consumer Protection, the Controller must retain the complaint for 3 years.

Legal basis for data processing: compliance with a legal obligation pursuant to Article 6(1)(c) of the Regulation or the Consumer Protection Act or the Civil Code.

Source of data: collected directly from the Data Subject.

Categories of recipients of personal data: database management partner, customer management

Possible consequences of refusing data disclosure: the complaint may not be handled, given that without providing personal data the Controller will not be able to establish and keep contact with the Data Subject and remedy the problem in connection with the given case.

No data transfer takes place outside the EU.

2.9. Newsletters, DM activities

Data being processed: surname, given name, email address.

The purpose of data processing: to record and identify the Data Subject in the newsletter database. In case of subscription, the Controller sends a newsletter with direct marketing content to the Data Subject by means of direct contact. In case of subscription, unless the Data Subject otherwise states, or objects to or protests against it, the Controller will use the personal data provided by the Data Subject during the subscription in order for the Controller to provide information about campaigns, offers and its services.

Duration of data processing: the Controller manages this data until the Data Subject unsubscribes from the newsletter by clicking on the unsubscribe link in the newsletter or until they request their removal by e-mail or post. After unsubscribing, the Controller will not contact the Data Subject with further newsletters or offers. The Data Subject may unsubscribe from the newsletter at any time, without restriction or reasons, free of charge.

Legal basis for data processing: the Data Subject's voluntary consent pursuant to Article 6(a) of the Regulation.

Source of data: collected directly from the Data Subject.

Categories of recipients of personal data: database management partner, marketing department

Possible consequences of refusing data disclosure: the Data Subject will not receive a newsletter with direct marketing content from the Controller, and will not have access to or be informed about discounted offers or promotion campaigns contained therein.

No data transfer takes place outside the EU.

2.10. Other personal information recorded by the system

Data being processed: IP address, type of browser.

The purpose of data processing: An identification number assigned by the ISP to the Data Subject's device logging into the system, the purpose of which is to ensure the security of the Controller's IT system as well as to send an html code corresponding to the type of browser.

Duration of data processing: The system will store the data for 6 months from the date of creation and then delete it automatically.

Legal basis for data processing: The Data Subject's voluntary consent pursuant to Article 6(1)(a) of the Regulation.

Source of data: collected directly from the Data Subject.

Categories of recipients of personal data: database management partner, marketing department

Possible consequences of refusing data disclosure: inaccuracy of analytical measurements.

3. DATA TRANSFER

Personal data may be accessed primarily by the Controller and the data processors entrusted by the Controller in order to perform their tasks. In addition, the Data Subject's personal data will be transferred to another data controller in the following cases.

The Controller hereby informs the Data Subject that the court, the Chief Attorney, the investigating authority, the offence authority, the public administration authority, the National Authority for Data Protection and Freedom of Information, and other public bodies authorised under the laws may request the Controller to disclose and/or deliver certain data and/or written documents.

The Controller may disclose personal data to the authorities only to such extent which is absolutely necessary for achieving the purpose of the data request, provided that the authority has specified the exact purpose and the scope of data requested.

The data provided by the Data Subject will not be transferred for any other purposes.

If the Data Subject chooses to pay by credit card on the Website, they will be redirected from the Website to the payment portal operated by the Hungarian Branch of Global Payments Europe s.r.o. The Controller will transmit the following data to the Hungarian Branch of Global Payments Europe s.r.o. as data controller: user name, surname, given name, country, phone number, e-mail address. The Hungarian Branch of Global Payments Europe s.r.o. does not transfer to the Controller the personal data received by it from the Data Subject during the payment process that is necessary for credit card payments. It only informs the Controller about the success or failure of the payment transaction.

Purpose of data transfer: to process payments by credit card, inform the Data Subject about the success or failure of the transaction by e-mail, and detect any frauds in order to protect the Data Subject (fraud detection system supporting the control of electronically initiated banking transactions).

Legal basis of data transfer: the Data Subject's voluntary consent pursuant to Article 6(1)(a) of the Regulation, given that online payment is only possible if the Data Subject consents to the transfer of data on the Website prior to the commencement of the credit card payment transaction.

4. ACCESS TO DATA, DATA SECURITY MEASURES, SECURITY BACKUPS

4.1. Data security measures

The Controller shall take all reasonably expected action to ensure the security of data and provide adequate protection in particular against unauthorised access, alteration, transfer, making public, deletion or destruction, as well as against accidental destruction or damage. The Controller shall ensure the security of the data by appropriate technical and organisational measures.

The IT system of the Website is hosted on the servers of Servergarden Korlátolt Felelősségű Társaság – DoclerNet Hosting.

The Controller shall choose and operate the information technology equipment used for providing its services related to the management of personal data so as to make sure that the data being managed:

- is accessible to those authorised to access the same (availability);
- its authenticity and authentication is secured (authenticity of data processing);
- its integrity can be verified (data integrity);
- it is protected against unauthorised access (confidentiality of data).

During the processing of data, the Controller shall maintain

- confidentiality: protect information from access by unauthorised persons;
- integrity: protect the accuracy and completeness of information and of the processing method;
- availability: make sure that whenever an authorised user needs it they can actually get access to the requested information and that the relevant equipment is also available.

4.2. The order of managing security backups

Within the framework of the tasks related to the security of IT systems, the Controller shall in particular take measures to ensure the possibility of restoring data files, including making regular backups and managing copies separately and securely (security backup).

Accordingly, in order to prevent the loss of electronically stored data, the Controller shall create daily, weekly and monthly backups of the data in its database, which also contain personal data, on a separate data storage device.

The retention period for security backups: 7 days for daily backups, 1 year for monthly backups.

Backups are deleted automatically by overwriting the previous backup.

Access to backups: access to backups is restricted to people with specific authorisation. Backups can only be restored in the event of system destruction or data loss, with the approval of the managing director from time to time.

5. DATA PROCESSING

The Controller is entitled, in accordance with the applicable laws, to employ a data processor for the purpose of certain technical operations or the provision of the service. The data processor is only entitled to execute the instructions and decisions of the Controller.

1. Novus Cura Kft.
Seat: 1048, Budapest, Székpatak utca 13.
Phone number: 06-30/2115881
E-mail: info@novuscura.hu
Activity: billing software operator
2. GLS General Logistics Systems Hungary Csomag-Logisztikai Kft.
Seat: 2351 Alsónémedi, GLS Európa u. 2.
E-mail: info@gls-hungary.com
Website: <https://gls-group.eu/HU/hu/home>
Activity: courier service, delivery partner
3. Computravel Bt.
Seat: 1048 Budapest, Székpatak utca 13.
Phone number: 06-30/2115881
e-mail: info@computravel.hu
Activity: IT system operator
4. PQRS Tanácsadó és Szolgáltató Kft.
Seat: 1048 Budapest, Intarzia utca 13.
Phone number: 06-20-402-0000
e-mail: iroda@piarsoft.hu
Activity: webshop developer / operator
5. Servergarden Korlátolt Felelősségű Társaság – DoclerNet Hosting
Seat: 1023 Budapest, Lajos utca 28-32.
Phone number: +3614323133
e-mail: info@servergarden.hu
Activity: hosting provider
6. Ferencvárosi Torna Club
Seat: 1091 Budapest, Üllői út 129.
Phone number: 061/91-00-241
e-mail: adatvedelem@fradi.hu
Activity: accountant, fan card data management
7. FTC Labdarúgó Zrt.

Seat: 1091 Budapest, Üllői út 129.
Phone number: 061/91-00-241
e-mail: adatvedelem@fradi.hu
Activity: accountant, fan card data management

6. RIGHTS OF THE DATA SUBJECTS

6.1. Information and access to personal data

The Data Subject may request written information from the Controller through the contact details provided in point 1 about the following:

- what personal data is being processed,
- on what legal basis,
- for what data processing purpose,
- from what sources,
- for how long,
- to whom, when, under what legislation, to which personal data of the Data Subject was granted access by the Controller or to whom such data was transferred.

If the Data Subject wishes to exercise their rights, this requires the identification of the Data Subject, and the Controller needs to communicate with the Data Subject. Therefore, to enable identification, it will be necessary to provide personal data (but the identification can only be based on data that is already processed by the Controller about the Data Subject), and the Data Subjects' complaints regarding data processing will be available in the Controller's e-mail account for the time period specified in this Notice for handling complaints.

Complaints related to data processing shall be answered by the Controller within the period set forth in point 6.8.

The Controller shall provide the information to the Data Subject in a widely used electronic format, unless the Data Subject requests it not electronically but on paper. The Controller does not provide verbal information by telephone regarding the personal data processed by it.

The Controller shall provide a copy of the personal data free of charge to the Data Subject for the first time. For any further copies requested from the Controller, the Controller may charge a reasonable fee based on its administrative costs. If the Data Subject requests the delivery of a copy electronically, the Controller shall deliver the same to the Data Subject by e-mail in a widely used electronic format.

After the information, if the Data Subject does not agree with the data processing and the correctness of the processed data, they may request the rectification, completion, deletion, restriction of processing, or object to the processing of such personal data, or may initiate the procedure referred to in point 6.

6.2. Right to rectify and complete the personal data being processed

At the written request of the Data Subject, the Controller shall, without undue delay, correct any inaccurate personal data indicated by the Data Subject in writing, or complete any incomplete data as requested by the Data Subject. The Controller shall notify all recipients about the rectification or completion to whom personal data has been disclosed, unless this proves impossible or involves a disproportionate effort. The Controller shall inform the Data Subject of the details of such recipients upon request in writing.

6.3. Right to restrict processing

The Data Subject may request the Controller in writing to restrict the processing of their data if:

- they contest the accuracy of the personal data, in which case the restriction shall apply for a period enabling the Controller to verify the accuracy of the personal data;
- the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead;
- The Controller no longer needs the personal data for the purposes of the processing, but they are required by the Data Subject for the assertion, exercise or defence of legal claims;
- the Data Subject objects to processing: in this case the restriction shall apply until it is verified whether the legitimate grounds of the Controller override those of the Data Subject.

Personal data subject to restriction shall, with the exception of storage, only be processed during the given period with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. The Controller shall notify the Data Subject who has obtained restriction of processing before the restriction of processing is cancelled.

6.4. Right to erasure (right to be forgotten)

The Data Subject has the right to obtain from the Controller the erasure of the Data Subject's personal data without undue delay if any of the following conditions apply:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed by the Controller;
- the Data Subject withdraws their consent and there is no other legal ground for data processing;
- the Data Subject objects to processing and there is no overriding legal ground (i.e. legitimate interest) for the processing;
- the personal data has been processed unlawfully and this has been established on the basis of the complaint;
- the personal data must be erased for compliance with a legal obligation in Union or Member State law to which we are subject.

Where the Controller has made your personal data public for any legitimate reason and was obliged to erase the same for any of the reasons listed above, the Controller, taking account of available technology and the cost of implementation, shall take all reasonably expected steps, including technical measures, to inform other controllers which are processing the personal data that you have requested the erasure by such controllers of any links to, or copy or replication of, those personal data. As a general rule, however, the Controller does not disclose the personal data of the Data Subject.

The data shall not be erased if data processing is required:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the Controller is subject (this includes data processing for invoicing purposes, because the retention of invoices is required by the law) or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- for the establishment, exercise or defence of legal claims (e.g. if we have a claim against the Data Subject which has not yet been satisfied or a consumer or data processing complaint is being processed).

6.5. Right to data portability

If the data processing is necessary for the performance of the contract or the data processing is based on the voluntary consent of the Data Subject, the Data Subject has the right to request that the data provided by the Data Subject to the Controller be transferred to them in a machine-readable form. The Controller shall provide the data to the Data Subject in xml, JSON or csv format, and if technically feasible, the Data Subject may request the Controller to transfer the data to another controller in one of the formats indicated above.

In any case, this right is limited to the data provided directly by the Data Subject, i.e. the portability option does not apply to any other data. (e.g. statistics, etc.)

The Data Subject shall be entitled with respect to the personal data stored in the Controller's system:

- to receive the data in an articulated, widely used, machine-readable format;
- to transfer the data to another data controller;
- to request the direct transfer of the data to another data controller if this is technically feasible in the Controller's system.

The Controller shall satisfy the request for data portability only on the basis of a written request submitted by e-mail or post. In order to satisfy the request, it is necessary for the Controller to make sure that the Data Subject who wishes to exercise this right is actually entitled to do so. Within the framework of this right, the Data Subject may request the portability of the data they have provided to the Controller. The exercise of this right does not automatically trigger the deletion of the data from the Controller's systems, therefore the Data Subject will continue to be recorded in the Controller's systems even after exercising this right, unless they also request the deletion of their data.

6.6. Right to object to processing of personal data

The Data Subject may object to the processing of their personal data by submitting a statement to the Controller if the legal basis for the data processing is

- in the interest of the public pursuant to Article 6(1)(e) of the GDPR or
- a legitimate interest pursuant to Article 6(1)(f) of the GDPR.

If the right to object has been exercised, the Controller shall stop processing the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. The Controller is entitled to determine whether the data processing is justified by compelling legitimate reasons. It shall inform the Data Subject of its position in this regard.

The Data Subject may object to the processing of their personal data only by a written request which must be sent to the Controller by e-mail or post.

6.7. Enforcement of the rights of deceased Data Subjects by another person

Within five years of the Data Subject's death, the rights that the deceased had as a Data Subject—e.g. the right to access, rectification, erasure, restriction of processing, data portability and objection—may be enforced by the person authorised by the deceased via an administrative order or through a declaration, to be made in a public document or in a private document with full probative force, given to the Controller. If the deceased made more than one such statement to the Controller, the person named in the statement last made may exercise these rights.

If the deceased has not made such a statement, the rights of the deceased as a data subject specified in the previous paragraph may be asserted by a close relative, as such term is defined in the Civil Code, of the Data Subject within five years after the death of the deceased Data Subject (in case of several close relatives, the one who exercises this right first).

Pursuant to paragraph 1 of Subsection (1) of Section 8:1 of the Civil Code, a close relative is the spouse, lineal relative, adopted, step and raised child, the adoptive, step and raising parent, and siblings. The deceased's close relative must prove:

- the fact and time of the death of the deceased Data Subject by a death certificate or a court decision, and
- the relative's own personal identity and, if necessary, their legal status as a close relative.

In exercising the above rights, in particular during the proceedings started against the Controller and before the National Authority for Data Protection and Freedom of Information or the court, the person exercising the rights of the deceased data subject shall have the same rights and obligations the data subject had pursuant to the Info Act and the Regulation when they were alive.

Upon written request, the Controller shall inform the close relative of the action taken unless the deceased has expressly prohibited this in their statement.

6.8. Deadline for satisfying the relevant request

The Controller shall provide information on action taken on a request to the Data Subject without undue delay and in any event within one month of receiving the request referred to in point 6. That period may be extended by two months where necessary, taking into account the complexity and number of the requests but in this case the Controller may notify the Data Subject within one month of receipt of the request about the reasons for the delay as well as about the Data Subject's right to file a complaint with the supervisory authority or to turn to court for remedy.

If the Data Subject's request is clearly unfounded or exaggerated (in particular due to its repetitive nature), the Controller may charge a reasonable fee for satisfying the request or refuse taking action on the request. It is the responsibility of the Controller to prove this.

Where the Data Subject makes the request by electronic means, the Controller shall provide the requested information by electronic means, unless otherwise requested by the Data Subject.

The Controller shall communicate any rectification or erasure of personal data or restriction of processing implemented by it to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves a disproportionate effort. The Controller shall inform the Data Subject about those recipients if the data subject requests so.

6.9. Indemnification and grievance fee

Any person who has suffered financial or non-financial loss as a result of a breach of the Regulation is entitled to compensation from the Controller or the data processor for the damage suffered. The data processor shall be liable for the damage caused by the processing only where it has not complied with its obligations specifically imposed on data processors in the relevant laws or where it has acted neglecting or contrary to the lawful instructions of the Controller. The Data Controller or the data processor shall be exempt from liability for damages if it proves that it is in no way responsible for the event giving rise to the damage.

7. AVAILABLE LEGAL REMEDIES

The Data Subject may exercise their rights by e-mail or a written request sent by post.

The Data Subject may not enforce their rights if the Controller proves that it is not in a position to identify the Data Subject. If the Data Subject's request is clearly unfounded or exaggerated (in particular due to its repetitive nature), the Controller may charge a reasonable fee for satisfying the request or refuse taking action. It is the responsibility of the Controller to prove this. Where the Controller has reasonable doubts concerning the identity of the natural person making the request, the Controller may request the provision of additional information necessary to verify the identity of the data subject.

Pursuant to the Info Act, the Regulation Civil Code (Act V of 2013), the Data Subject may

- turn to the Hungarian National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa u. 9-11.; www.naih.hu), or
- enforce their rights before court. The Data Subject may choose to start the action at the court that has jurisdiction according to the Data Subject's place of residence. (You can view the list and contact details of the relevant courts via the following link: <http://birosag.hu/torvenyszekek>).

8. HANDLING DATA BREACHES

'Data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the personal data transmitted, stored or otherwise processed. In order to control the measures taken in response to a data breach and to inform the supervisory authority and the Data Subject, the Controller shall keep a register containing the scope of personal data affected by the data breach, the date, circumstances and effects of the incident, and the measures taken. In case a data breach has occurred, except where it does not jeopardize the rights and freedoms of natural persons, the Controller shall inform the Data Subject and the supervisory authority of the data breach without undue delay and within a maximum of 72 hours.

9. MISCELLANEOUS PROVISIONS

The Controller reserves the right to unilaterally amend this Privacy Notice with prior notice to the Data Subject, including but not limited to amendments in case of changes in legislation. The amendment shall enter into force for the Data Subject on the date specified in the notice, unless the Data Subject objects to the amendment.

If the Data Subject has provided the data of a third party for using the service, by which they have caused damage in any way, the Controller is entitled to enforce indemnification against the Data Subject.

The Controller does not check the personal data submitted to it. The person providing the personal data shall be solely responsible for the correctness of such data. When providing their personal data, the Data Subject is also responsible for ensuring that the data provided is true, it is their own personal data and that only they are using the service with such data.

The Controller reserves the right to amend this Privacy Notice in a manner that does not affect the purpose and legal basis of the data processing.

However, if we wish to carry out further data processing in connection with the collected data for a purpose other than the one for which they were originally collected, we will inform you about such purpose of data processing and the following information before any further data processing:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,

- your rights to request from the Controller access to and rectification or erasure of your personal data or restriction of processing concerning the personal data and to object to processing in case the processing is based on a legitimate interest as well as the right to data portability in case the processing is based on consent or a contractual relationship;
- in case of data processing based on your consent, that you may withdraw your consent at any time,
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a condition precedent to the conclusion of a contract, as well as whether you are obliged to provide the personal data and of the possible consequences of failure to provide such data;
- whether automated decision-making including profiling (if any) is applied and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you.

The Controller may start data processing only after this, and if the legal basis of the data processing is your consent, you must also consent to the data processing in addition to the above information.

If you have any further questions or issues with data processing, please write an e-mail to marketing@fradi.hu.