**FINNOVATIVE SOLUTIONS UAB**
**RULES FOR THE PROCESSING OF PERSONAL DATA**

## CHAPTER I
## GENERAL PROVISIONS

1.1. The rules of personal data processing of Finnovative Solutions UAB (hereinafter - the Rules) regulate the principles of personal data processing of natural persons whose data are processed by Finnovative Solutions UAB (hereinafter - the company), establish the procedure for implementation of their rights, establish organizational and technical data protection measures, procedures for managing personal data security breaches, data protection implications, staff monitoring and the functions of personal data controllers.

1.2. The following personal data of data subjects are processed in the company in manually organized files and / or automatically:

1.2.1. personal data of data subjects in the company's information systems, the purpose of processing and the exhaustive list of processed personal data of which are provided in the legal acts of the Republic of Lithuania regulating the functions of the payment institution and / or in the company's personal data processing activity records acts;

1.2.2. personal data of the users of the company's electronic service portals (name, surname, date of birth / personal code).

1.3. The data controller of the personal data specified in sub-paragraphs 1.2.1–1.2.2 of the Rules is Finnovative Solutions UAB, legal entity code 305206391, registered office address: Upės str. 23, LT-08128, Vilnius.

1.4. When processing personal data, the company shall follow the personal data processing requirements established in the Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter - ADTAĮ), General Requirements for Organizational and Technical Personal Data Security Measures approved by the Director of the State Data Protection Inspectorate in 2008. November 12 by order no. 1T-71 (1.12) "On the Approval of General Requirements for Organizational and Technical Measures for the Security of Personal Data" (hereinafter referred to as the "General Requirements") and other legal acts related to the processing and protection of personal data, General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as BDAR).

1.5. These Rules must be complied with by data processors who, in providing data processing services to the Company, find out and process personal data.

## CHAPTER II
## BASIC CONCEPTS

2.1. Personal data - shall mean any information relating to an identified or identifiable natural person, directly or indirectly, in particular by means of an identifier such as name, surname, personal code / birth date.

2.2. Processing data - means any operation or sequence of operations carried out by automated or non-automated means on personal data or personal data sets, such as collection, recording, sorting, systematisation, storage, adaptation or modification, retrieval, access, use, disclosure, transfer, distribution or otherwise making them available, as well as collating or merging with other data, limiting, deleting or destroying them.

2.3. Data controller - Finnovative Solutions UAB, which, when processing the data of interested parties, other natural persons, determines the methods and means of using that data.

2.4. Data subject – applicants / customers, interested parties and other natural persons whose data are processed by Finnovative Solutions UAB.

2.5. Data processor - entities that process Personal Data managed by Finnovative Solutions UAB in accordance with the instructions of Finnovative Solutions UAB and follow the concluded service agreements.

2.6. Provision of data - Disclosure of personal data through transmission or other making available (excluding publication in the media).

2.7. Internal administration - activities that ensure the independent functioning of the data controller (structure management, personnel management, management and use of financial resources, clerical management).

2.8. Other terms used in the Rules shall be understood as they are defined in the ADTAĮ and / or BDAR.

## CHAPTER III
## PRINCIPLES OF DATA PROCESSING

3.1. Implementing independent functions, the Company's divisions process personal data in accordance with their competence to perform the provided services, perform internal administration functions.

3.2. Time limits for the storage of personal data and actions to be taken after the expiry of this time limit shall be established by legal acts regulating the processing of personal data. Personal data shall be kept for no longer than is necessary for the purposes of the processing. Specific time limits for the storage of personal documents (data) may be set out in the documentation plan approved by the Company's Director and in the data processing rules of the relevant Company's unit must be transferred to the state archives in accordance with the established procedure.

## CHAPTER IV
## RIGHTS OF DATA SUBJECTS AND PROCEDURES FOR THEIR ENFORCEMENT

### *GENERAL PROVISIONS*

4.1. Data subjects have the following rights enshrined in the BDAR:
- 4.1.1. the right to know (be informed) about the processing of your personal data in the Company;
- 4.1.2. the right to access your personal data processed in the Company;
- 4.1.3. the right to have personal data rectified;
- 4.1.4. the right to request the deletion of personal data (the right to be forgotten);
- 4.1.5. the right to restrict the processing of personal data;
- 4.1.6. the right to object to the processing of personal data;
- 4.1.7. the right to portability of personal data;
- 4.1.8. the right to restrict data processing;
- 4.1.9. the right to withdraw consent freely and without hindrance.

4.2. In all cases, when implementing the rights of data subjects specified in these Rules, the Company must provide the data subject with the following information (except in cases when the data subject already has such information):
- 4.2.1. its name, legal entity code and registered office;
- 4.2.2. contact details of the company's data protection officer (if any);
- 4.2.3. the purposes and legal basis of which the personal data of the data subject are processed;
- 4.2.4. data recipients;
- 4.2.5. the data retention period or the criteria used to define that period;
- 4.2.6. other additional information (sources of data, what personal data the data subject must provide and what are the consequences of not providing the data, the data subject's right of access to his personal data and the right to request the correction of incorrect, incomplete, inaccurate personal data), to the extent necessary, to ensure the correct processing of personal data without violating the rights of the data subject, as well as information on the right of the data subject to lodge a complaint with the State Data Protection Inspectorate;

4.3. The company should also:
- 4.3.1. to enable the data subject to exercise the rights of the data subject specified in these Rules, except for cases established by legal acts when it is necessary to ensure state security or defence, public order, prevention, investigation, detection or prosecution of criminal offenses, important economic or financial interests of the state; or the prevention, investigation and detection of breaches of professional ethics, the protection of the rights and freedoms of the data subject or of other persons;
- 4.3.2. data subjects shall apply to the Director of the Company regarding the implementation of the rights specified in these Rules;

4.3.3. the company must ensure that all necessary information is provided to the data subject in a clear and comprehensible manner;

4.3.4. the response must be provided to the data subject no later than within 30 calendar days from the date of receipt of the request by the Company. This period may be extended by a further two months depending on the complexity of the application and the number of applications pending. The company must, within 30 calendar days from the date of receipt of the request, inform the data subject about the extension of the deadline for processing the request and provide the reasons for the extension;

4.3.5. the undertaking shall have the right to refuse to provide the data subject with the information it requests if the data subject's request is manifestly unfounded or disproportionate. If the data subject is refused, he or she must be provided with a reasoned and reasoned reply for not complying with his or her request.

4.4. The company must immediately, but not later than within 5 days, inform the data recipients about personal data corrected or destroyed at the request of the data subject, suspended personal data processing activities, unless it would be impossible or excessively difficult to provide such information (due to the large number of data subjects, data period, unreasonably high costs). In this case, the State Data Protection Inspectorate must be notified immediately, but not later than within 3 working days.

4.4.1. the company shall provide the data to the data subject free of charge, except for any other copies of the data requested by the data subject and other cases established by legal acts, taking into account the administrative costs incurred in the implementation of the request.

***RIGHT TO KNOW (BE INFORMED) ABOUT THE PROCESSING OF YOUR PERSONAL DATA***

4.5. The right to know (be informed) about the processing of one's personal data is exercised in the following ways:

4.5.1. informing data subjects that the oral consultations provided by the Company by telephone will be recorded;

4.5.2. informing users connecting to the Company's electronic services management system for the first time about the processing of personal data;

4.5.3. providing information on the Company's website, etc.;

4.5.4. during communication with the data subject in the manner in which the data subject applies to the Company;

4.5.5. in other ways, taking into account the nature and specificity of the data processing operations carried out.

4.6. When data are collected from data subjects, in order to exercise the data subjects' right to be informed about the processing, the data subject must be provided with all the information specified in Article 13 of the BDAR.

4.7. Where personal data are not obtained from the data subject, all data referred to in Article 14 of the BDAR shall be provided to the data subject in accordance with the deadlines specified in Sub-paragraph of these Rules.

4.8. The enterprise has the right to refuse to exercise the data subject's right provided for in Sub-paragraph of these Rules or to provide incomplete information requested by the data subject, if:

4.8.1. the data subject already has this information;

4.8.2. the provision of the information requested by the data subject is not possible or would require a disproportionate effort;

4.8.3. the receipt or disclosure of personal data is clearly established in the legal acts of the European Union or in the legal acts of the Republic of Lithuania, which establish appropriate measures for the protection of the interests of lawful data subjects;

4.8.4. personal data must remain confidential, in compliance with the obligation of professional secrecy regulated by the legal acts of the European Union or the legal acts of the Republic of Lithuania.

## *EXERCISE OF THE RIGHT OF ACCESS TO YOUR PERSONAL DATA*

4.9. In accordance with the procedure established by these Rules, a data subject who has confirmed his or her identity or his or her representative shall have the right, free of charge:

4.9.1. to get acquainted with his / her data processed in the Company;

4.9.2. to receive information from which sources and what personal data have been collected;

4.9.3. to find out the purpose for which his personal data is processed;

4.9.4. the intended period of retention of personal data or the criteria for determining the period of retention of personal data;

4.9.5. if possible, to which recipients their personal data have been supplied in the last one year.

4.10. If the Company handles a large amount of information related to the data subject and it is not possible to provide all the information to the data subject, the Company has the right to ask the data subject to specify the submitted request:

4.10.1. where certain information about the data subject also relates to other persons, the information must be provided to the data subject to the extent that the rights of other persons are not infringed.

4.10.2. information on personal data processed by the data subject The Company shall submit to the data subject upon completion of the application for access to personal data, the form of which is provided in Annex 1 to the Rules.

4.10.3. the response to the data subject must be provided in writing.

## *EXERCISE OF THE RIGHT TO REQUEST THE CORRECTION OF PERSONAL DATA*

4.11. If the data subject, having acquainted himself with his personal data, determines that his personal data is incorrect, inaccurate or incomplete and applies to the Company, the Company shall immediately, but not later than within 5 working days, verify the personal data and the data subject's written request personally, by post or by electronic means of communication, immediately correct incorrect, inaccurate or incomplete personal data processed by the Company and (or) suspend the processing of such personal data, except for storage until incorrect, inaccurate and incomplete personal data is corrected or personal data is destroyed.

4.12. The company shall immediately, but not later than within 3 working days, notify the data subject about the rectification, destruction or suspension of personal data processing actions performed or not performed at the request of the data subject. The company shall also immediately inform the recipients of personal data rectified or destroyed at the request of the data subject, suspended personal data processing operations, unless it would be impossible or excessively difficult to provide such information (due to the large number of data subjects, data period, unreasonable costs). In this case, the Company shall immediately, but not later than within 3 working days, notify the State Data Protection Inspectorate.

## *EXERCISE OF THE RIGHT OF DISPUTE TO THE PROCESSING OF PERSONAL DATA*

4.13. Methods of implementation:

4.13.1. the data subject who consents to the processing of his or her personal data must provide a written notice of objection to the processing of personal data. Notification to the Company may be made directly, by registered mail or by electronic means;

4.13.2. where the data subject's personal data are processed for the legitimate interests of the Company (or providing data to third parties), the Company must contact the data subject in writing and set a reasonable time limit to exercise the data subject's right to object to the processing, through which the data subject has the right to object to the processing, for example to the disclosure of his data to a third party;

4.13.3. if the consent of the data subject is legally justified, the Company shall immediately terminate the processing of personal data, except in cases prescribed by legal acts, and shall inform the recipients of the data whenever possible. If the request is unfounded, the Company shall indicate in writing to the data subject the reasons why the personal data of the data subject must continue to be processed for justified and lawful reasons which outweigh the interests of the data subject;

4.13.4. if the data subject has not submitted a written notice of disagreement regarding the processing of personal data by the deadline set by the Company, it shall be deemed that the data subject has not expressed consent to the processing of his or her personal data;

## *EXERCISE OF THE RIGHT TO REQUEST THE DELETION OF YOUR PERSONAL DATA*

4.14. Data subjects have the right to demand the deletion (right to be forgotten) of their personal data or to restrict the processing of data, except for storage, when the data is processed in violation of the requirements of legal acts. This right is valid on one of the following grounds:

4.14.1. personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

4.14.2. the data subject revokes the consent on which the processing was based and there is no other legal basis for the processing;

4.14.3. personal data have been processed illegally;

4.14.4. personal data must be deleted in accordance with a legal obligation under European Union or national law.

4.15. The data subject's request must contain a detailed argumentation of the reasons for which the deletion of his or her personal data is requested (the request must specify one of the grounds specified in these Rules).

4.16. The right to request the deletion of personal data (right to be forgotten) is not exercised in the Company when the processing of personal data is based on:

4.16.1. compliance with the requirements established in the legal acts of the European Union and the Republic of Lithuania;

4.16.2. for archival purposes in the public interest;

4.16.3. to express, exercise or defend legal interests.

4.17. Upon receipt of the data subject's request, the undertaking shall immediately, but not later than within 10 working days from the date of receipt of the request, perform an assessment of the request in order to determine whether the data subject's request is justified.

4.18. If it is established that the request submitted by the data subject is justified, the Company must:

4.18.1. immediately, but not later than within 5 working days, delete all available personal data related to the data subject;

4.18.2. if it is not possible to immediately delete the personal data of the data subject, suspend the processing of personal data of the data subject;

4.18.3. to inform the data subject about the deleted personal data no later than within 5 working days from the deletion of personal data;

4.18.4. to inform the data recipients about the personal data deleted at the request of the data subject, if the personal data of the data subject were provided to the data recipients. It is not necessary to inform data recipients when it is not possible or too difficult to provide such information (due to the large number of data subjects, the retention period of personal data, unreasonably high costs).

## *EXERCISE OF THE RIGHT TO REQUEST TRANSFER OF PERSONAL DATA*

4.19. The data subject or his / her representative has the right to apply to the Company with a request to receive personal data related to him / her and has the right to request the transfer of personal data of the data subject processed in the Company to another data controller when:

4.19.1. data processing is performed with the consent of the data subject or performed by an agreement between the Company and the data subject;

4.19.2. personal data is processed by automated means;

4.19.3. the data subject has provided the Company with the personal data that he / she intends to transfer to another data controller himself / herself or through a representative;

4.19.4. the personal data provided by the data subject are systematised and presented in a commonly used and computer-readable format.

4.20. Upon receipt of a request from a data subject to exercise the data subject's right, an undertaking shall immediately, but not later than within 10 working days from the date of receipt of the request, assess the request to determine whether the request submitted by the data subject is justified. If the request is justified, the information may be provided - the data subject. To another controller if:

4.20.1. the data subject indicates in the request that the Company should transfer the personal data to another data controller;

4.20.2. there are technical possibilities to provide personal data directly to another controller.

4.21. If the data subject's request for transfer of personal data is implemented by transferring the data subject's personal data to another data controller, the Company does not assess whether the data controller to whom the data subject's personal data will be transferred has a legal basis to receive the data subject's personal data. personal data security measures. The company does not take responsibility for the further processing of the transferred personal data by another data controller.

4.22. The undertaking shall ensure that, in the exercise of their right to data portability by data subjects, only data which are processed on the basis of a contract or consent and which are processed by automated means are transferred. In this case, the personal data would be provided to the data subject in a structured, commonly used and computer-readable format.

4.23. The data subject's right to data portability will not apply in cases where the processing of personal data is necessary for the Company to comply with a legal obligation imposed on it or to perform a task performed in the public interest.

## *EXERCISE OF THE RIGHT TO RESTRICT THE PROCESSING OF OWN PERSONAL DATA*

4.24. The data subject has the right to apply to the Company with a request to restrict the processing of his / her personal data if one of the following grounds exists:

4.24.1. the data subject disputes the accuracy of his personal data processed by the Company. In that case, the processing of the data subject's personal data may be limited to the period during which the controller verifies the accuracy of the personal data;

4.24.2. it is established that the processing of the data subject's personal data has been unlawful, but the data subject does not consent to the deletion of the personal data, but instead requests that their processing be restricted;

4.24.3. if the purpose of processing personal data has been achieved and the Company, as the data controller, no longer needs the personal data of the collected data subject to achieve this purpose, but they are needed by the data subject to express, enforce or defend legal claims;

4.24.4. the data subject submitted a request to the Company in which he expressed his disagreement that the Company would process his personal data. In that case, the processing of the data subject's personal data may be limited to the period during which the controller verifies that the data subject's request is justified;

4.24.5. the data subject submits a request to delete the personal data processed by the Company and it is established that the request is justified, but there is no technical possibility to delete the personal data of the data subject immediately. In this case, the processing of the data subject's personal data may be restricted until the data subject's personal data have been deleted.

4.25. Upon receipt of a request from a data subject, an undertaking shall immediately, but not later than within 10 working days from the date of receipt of the request, perform an assessment of the request in order to determine whether the request submitted by the data subject is justified. If it is established that the request submitted by the data subject is justified, the Company must:

4.25.1. restrict the processing of personal data of the data subject;

4.26. When a decision is made to lift a restriction on the processing of personal data of a data subject, the Company must inform the data subject in writing before lifting the restriction.

## *PROVISION OF DATA TO RECIPIENTS*

4.27. The enterprise shall provide the data of data subjects to the data recipients only in accordance with the concluded contract or a one-time request of the data recipient, without prejudice to the requirements established by legal acts and ensuring the confidentiality of personal data.

4.28. In case of one-time data provision, the Company, when providing personal data at the request of the data recipient, gives priority to the provision of data by electronic means of communication.

4.29. Data may be provided when the recipient of the data indicates in the submitted request:

4.29.1. the specific and clearly defined purpose of obtaining the data;

4.29.2. the legal basis for obtaining the data;

4.29.3. the legal basis for the provision of data, specified in the BDAR, according to which the Company has the right to provide this data to the data recipient;

4.29.4. the specific scope of the data;
4.29.5. when data are requested in accordance with Article 6 (1) (e) or (f) of the BDAR, i.e. the data must be provided for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in order to protect the legitimate interests of the controller or a third party, the request must state why those interests outweigh those of the data subject.

4.30. If you have questions / requests with your data processed by the company, you can fill in the form set out in Annex 1 to these rules by sending it directly email: gdpr@finnovative.eu.

4.31. The contact details of the official are published on the Company's website http://finnovative.eu/.

## CHAPTER V
## DATA PROTECTION IMPACT ASSESSMENT

5.1. When an undertaking starts new data processing operation (s), it must carry out a data protection impact assessment if the processing:
5.1.1. would seriously jeopardize the rights and freedoms of data subjects (for example, the transfer of data outside the European Union or the processing of data obtained by combining data from other sources, the introduction of new technological solutions such as facial recognition systems), etc.);
5.1.2. automated processing of personal aspects, profiling and legal or other decisions with significant implications (for example, where the processing of data may lead to the exclusion or discrimination of individuals);
5.1.3. large-scale processing of sensitive personal data.

5.2. If the Company, during the data protection impact assessment, determines that the rights and freedoms of data subjects may be seriously endangered, it must consult with the State Data Protection Inspectorate on the implementation of appropriate security and other measures.

5.3. In performing the data protection impact assessment, the Company must determine:
5.3.1. what data processing operation (s) will be performed;
5.3.2. the extent to which a specific data processing operation is necessary and proportionate;
5.3.3. what the impact may be on data subjects;
5.3.4. what are the possible measures for elimination of potential dangers, ensuring security.

5.4. The Company must ensure that the data protection impact assessment described in this Chapter and performed by the Company in the cases provided for is properly documented and stored.

5.5. Data protection impact assessments may also be carried out for existing data processing operations if there are significant changes in those operations, such as the introduction of new technologies, data processing for a different purpose, new risks, related to the

performed cyber-attacks, intrusions into the Company's system, the data would be provided to new data recipients, processors outside the European Union, etc.

5.6. The data protection impact assessment may also be performed in cases not discussed in this Chapter, but upon the recommendation of the Director, official or the State Data Protection Inspectorate.

## CHAPTER VI
## MANAGEMENT OF PERSONAL DATA BREACHES

6.1. A personal data breach is any intentional or negligent personal data breach when:
- 6.1.1. personal data is destroyed, lost or altered;
- 6.1.2. personal data is disclosed without permission;
- 6.1.3. unauthorized persons would have access to personal data without permission.

6.2. If the violation of personal data security endangers the rights and freedoms of data subjects, the official appointed by the Director of the Company must immediately, but not later than within 72 hours, notify the State Data Protection Inspectorate about the data security violation. If the personal data security breach is not reported to the State Data Protection Inspectorate within 72 hours, the reasons for the delay must be attached to the notification.

6.3. In the event of a particularly serious threat to the rights and freedoms of data subjects, information on the breach of security must also be provided to the data subjects without delay. If it is not possible to inform all data subjects due to their large number or other reasons, the official together with the Director of the Company considers and makes a decision to provide this information through the media.

6.4. In the event of a personal data breach discussed in this Chapter of the Rules, the Officer shall, among other responsibilities discussed in this section, draw up an action plan with preventive actions to prevent similar data breaches in the future and submit it to the Company's Director.

## CHAPTER VII
## TECHNICAL AND ORGANIZATIONAL MEASURES FOR THE PROCESSING OF PERSONAL DATA

7.1. These General Requirements for Organizational and Technical Data Security Measures of the Company establish general requirements for organizational and technical data security measures to protect personal data from accidental or unlawful destruction, alteration, disclosure, as well as from any other unlawful processing.

7.2. Depending on the nature of the personal data to be stored and the risks involved in their processing, three levels of security of personal data processed automatically are distinguished.

7.3. The organizational and technical data security measures of the enterprise shall ensure the second level of security of personal data processed automatically, except in cases when the implementation of the third level of security is mandatory.

7.4. In order to protect personal data from accidental or unlawful destruction, alteration, disclosure, or any other unlawful processing, the following infrastructural, administrative and telecommunication (electronic) measures shall be applied:

7.4.1. secure and proper placement and maintenance of hardware, maintenance of information systems (IS), network (LAN, wireless) management, security of Internet use and other information technology measures;

7.4.2. safe and proper organization of work and other administrative measures;

7.4.3. practical tests are performed for disaster recovery of personal data;

7.4.4. data backup is performed at least once a month;

7.4.5. ensure data recovery from the latest available backup data in case of data loss due to hardware failure, software error or other data integrity violation;

7.4.6. performing IS functionality and data integrity and readiness testing;

7.4.7. a pilot data recovery must be performed at least once a year.

## CHAPTER VIII
## PROCEDURE FOR KEEPING DATA ACTIVITY RECORDS

8.1. The procedure for keeping records of data activities in the Company is used in accordance with the following principles:

8.1.1. must be used strictly for work purposes only;

8.1.2. the use must ensure compliance with confidentiality obligations, intellectual property rights, including the rights and legitimate interests of third parties, and general ethical and moral principles.

8.2. The procedure for keeping records of data activities shall be reviewed at least once a year and, if necessary or amended, the legal acts regulating the processing of personal data shall be updated by implementing structural, technological or other changes. An official of the Company is responsible for the supervision of the observance of the provisions of this Procedure and the control of the implementation of the provisions regulated therein, and the initiation of renewal as required.

8.3. All actions not provided for in this Chapter related to the keeping of records of data activities in the Company must be coordinated with an official of the Company.

## CHAPTER IX
## FINAL PROVISIONS

9.1. The Rules shall be reviewed at least once every 2 years and, if necessary or changed, the legal acts regulating the processing of personal data shall be updated. Compliance with the provisions of these Rules shall be monitored and, if necessary, updated by an official of the Company.

9.2. The actions and decisions of the entities implementing the Rules may be appealed in accordance with the procedure established by legal acts.

Rules for the processing of personal data
Annex 1

***(Personal data request form)***

To the director of
Finnovative Solutions UAB

**REQUEST FOR ACCESS TO PERSONAL DATA**

_____
date
Vilnius

Pursuant to Article 15 of the General Data Protection Regulation (hereinafter - BDAR), you have the right to receive a copy of the personal data that Finnovative Solutions UAB (hereinafter - the company) has about you. Information on how the company handles your personal data will be provided to you no later than 30 calendar days after your written request.

All requests must be made in writing and contain sufficient information to enable the company to properly identify: You as a data subject; and information about you. To help us respond effectively to your inquiry, please provide the company with the following information in writing. You can fill out this form and return it to us:

| Nr. | Description | To be completed by the applicant |
|---|---|---|
| 1. | Name, surname (required) | |
| 2. | address | |
| 3. | Email address | |
| 4. | | |

In order to make our search faster, please provide as much data as possible about the information you request and, if possible, where that information could be stored.

Description of information requested:

Specify a specific time period:

□ Check this box to get a copy of all available personal data.
□ Check this box to receive an electronic copy of all personal data you hold.
I certify that all personal data I request is provided. Please send the completed and signed form by e-mail or post to the following address: Upės g. 23, LT-08128 Vilnius.

_____ _____
*(signature)* *(name, surname)*