FINNOVATIVE SOLUTIONS UAB
RULES FOR THE PROCESSING OF PERSONAL DATA

CHAPTER I
GENERAL PROVISIONS

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.
2. The Personal Data Controller of the Personal Data specified in the Rules-is Finnovative Solutions UAB, legal entity code 305206391, registered office address: Laisvės pr. 60-308 LT-05120, Vilnius. The contact details of the Personal Data Administrator are:
    a) address for written correspondence: Laisvės pr. 60-308 LT-05120 Vilnius, Lithuania
    b) address for electronic correspondence: support@finnovative.eu
3. 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: "**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: "**GDPR**").
4. 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

1. **AIS –** shall mean an online service to provide consolidated information on one or more payment accounts held by the Payment Services User with either another payment service provider or with more than one payment service provider provided by Personal Data Controller.
2. **Data Subject** – shall mean a Payment Service Users interested parties and other natural persons whose data are processed by Finnovative Solutions UAB.
3. **Data processor –** shall mean an 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.
4. **Internal administration** – shall mean a activities that ensure the independent functioning of the data controller (structure management, personnel management, management and use of financial

resources, clerical management).

5. **Partner –** an entity that cooperates with the Personal Data Controller on the basis of a separately concluded cooperation agreement, the Subject of which is the provision of payment services by the Personal Data Controller to the Partner's clients and which provides the Personal Data to the Personal Data Controller for processing by the Personal Data Controller for the purposes indicated by the Personal Data Controller.
6. **Payment Services** – shall mean a both AIS and PIS provided by the Company.
7. **Payment Services User** – shall mean a Partner's client using Payment Services provided by Personal Data Controller on the basis of a separate one-time agreement for the provision of payment services concluded with the Payment Service User.
8. **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.
9. **PIS –** shall mean a service to initiate a payment order at the request of the Payment Service User with respect to a payment account held at another payment service provider by Personal Data Controller.
10. **Processing data –** shall mean 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.
11. **Personal Data Controller –** shall mean a Finnovative Solutions UAB, which, when processing the data of interested parties, other natural persons, determines the methods and means of using that data.
12. **Provision of data** – shall mean a disclosure of Personal Data through transmission or other making available (excluding publication in the media).
13. Other terms used in the Rules shall be understood as they are defined in the ADTAĮ and / or GDPR.

CHAPTER III
PRINCIPLES OF DATA PROCESSING

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.
2. Time limits for the storage of Personal Data and actions to be taken after the expiry of thistime 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 Rules. The Rules of data processing by the relevant units of the Company may be transferred to state archives in accordance with the established procedure and provisions of Lithuanian law.

CHAPTER IV
THE PURPOSES OF THE PROCESSING OF PERSONAL DATA

1. The Personal Data Administrator processes the Personal Data of Payment Service Users for the following purposes:
    a) In order to execute of the contract for the provision of Payment Services - including the

performance of obligations arising from this contract, including the consideration of complaints - the legal basis is the necessity of processing to take action before concluding the contract and for the purpose of performing the contract (Article 6(1)(b) of the GDPR);

b) in order to provide Personal Data to the Partner - based on your consent to provide them (Article 6(1)(a) of the GDPR)- when using the AIS service;

c) In order to perform obligations arising from legal provisions, including provisions governing the provision of Payment Services, tax law, accounting and financial reporting regulations - the legal basis is the necessity to perform obligations arising from legal provisions (Article 6(1)(c) of the GDPR);

d) In order to establish, pursue or defend against claims - the legal basis is the necessity of processing to perform the contract (Article 6(1)(b) of the GDPR) or the Personal Data Controller's legitimate interest (Article 6(1)(f) GDPR), where the legitimate interest is the exercise of rights.

2. Personal Data will not be processed in an automated manner, including profiling.

CHAPTER V

SCOPE OF PERSONAL DATA

1. When performing Payment Services, the Personal Data Administrator processes the following Personal Data of the Payment Services User:
   a) in the case of performing the PIS service:
      - Name, surname;
      - E-mail address;
      - Account number;
      - IP number;
      - Name of Payment Service User’s company (if the Payment Services User is a legal person or an organizational unit without legal personality);
      - Tax identification number;
   b) In the case of performing the AIS service:
      - Name, surname;
      - Name of Payment Service User’s company (if the Payment Services User is a legal person or an organizational unit without legal personality);
      - E-mail address.

CHAPTER VI

RECIPIENTS OF THE PERSONAL DATA

1. The Company shall provide the data of Payment Service Users 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. In particular, when using the AIS service, we may share Personal Data with Payment Service User to the Partner in accordance with the agreement concluded with Payment Service User.
2. 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 ofcommunication.
3. The Company may transfer Personal Data to entities processing Personal Data on behalf of the Company, i.e. IT and e-mail service providers, technology providers, accountants, entities dealing with the destruction of data media.

4. The entity processing Personal Data in the scope of providing Payment Services is, in particular, Savangard sp z o.o. based in Warsaw, with which the Company concluded an agreement entrusting the performance of activities as part of the Payment Services provided.
5. Personal Data may also be transferred to entities authorized to request this data under applicable regulations.
6. Personal Data shall not be transferred to recipients outside the European Economic Area (EEA).

CHAPTER VII
RIGHTS OF DATA SUBJECTS AND PROCEDURES

GENERAL PROVISIONS

Data Subject s have the following rights enshrined in the GDPR:

a) the right to know (be informed) about the processing of your Personal Data in the Company;
b) the right to access your Personal Data processed in the Company;
c) the right to have Personal Data rectified;
d) the right to request the deletion of Personal Data (the right to be forgotten);
e) the right to restrict the processing of Personal Data;
f) the right to portability of Personal Data;
g) the right to withdraw consent freely and without hindrance;
h) the right to object to the processing of Personal Data.

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

1. The right to know (be informed) about the processing of one's Personal Data is exercised in the following ways:
   a) informing Data Subject s that the oral consultations provided by the Company by telephone will be recorded – if the Company provides such a possibility;
   b) informing the Payment Services User who each time connects to the Company's electronic services management system about the processing of personal data;
   c) providing information on the Company's website;
   d) informing of processing the Personal Data during communication with the Data Subject in the manner in which the Data Subject applies to the Company;
   e) informing of processing the Personal Data in other ways, taking into account the nature and specificity of the Personal Data processing operations carried out.
2. The Company 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:
   a) the Data Subject already has this information;
   b) the provision of the information requested by the Data Subject is not possible or would require a disproportionate effort;
   c) 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 Subject's;

d) Personal Data must remain confidential, in compliance with the obligation of professional secrecy regulated by the legal acts of the European Union or the legalacts of the Republic of Lithuania.

EXERCISE OF THE RIGHT OF ACCESS TO YOUR PERSONAL DATA

1. In accordance with the procedure established by these Rules, a Data Subject shall have the right, free of charge:
   a) to get acquainted with his / her Personal Data processed in the Company;
   b) to receive information from which sources and what Personal Data have been collected;
   c) to find out the purpose for which his Personal Data is processed;
   d) where possible, get the information about the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period; the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organisations;
   e) to get information about the existence of the right to request from the Personal Data Controller rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing;
   f) to get information about the right to lodge a complaint with a supervisory authority;
   g) to get information about the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR 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 the Data Subject.
2. 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.
3. 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 Subject s, 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 (Valstybinė duomenų apsaugos inspekcija).
4. Submitting a request for access to Personal Data may be made using the template form from Annex 1.

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

1. Data Subject s 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:
    a) Personal Data are no longer necessary for the purposes for which they were collected or otherwise processed;
    b) the Data Subject revokes the consent on which the processing was based and thereis no other legal basis for the processing;
    c) Personal Data have been processed illegally;
    d) Personal Data must be deleted in accordance with a legal obligation under EuropeanUnion or national law.
2. 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).
3. The right to request the deletion of Personal Data (right to be forgotten) is not exercised inthe Company when the processing of Personal Data is necessary to:
    a) compliance with the requirements established in the legal acts of the EuropeanUnion and the Republic of Lithuania;
    b) for archival purposes in the public interest;
    c) to express, exercise or defend legal interests.
4. 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.
5. If it is established that the request submitted by the Data Subject is justified, the Company must:
    a) immediately, but not later than within 5 working days, delete all available Personal Data related to the Data Subject;
    b) 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;
    c) to inform the Data Subject about the deleted Personal Data no later than within 5 working days from the deletion of Personal Data;
    d) 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 toodifficult to provide such information (due to the large number of Data Subject s, the retention period of Personal Data, unreasonably high costs).

EXERCISE OF THE RIGHT TO REQUEST TRANSFER OF PERSONAL DATA

1. The Data Subject 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 transferof Personal Data of the Data Subject processed in the Company to another data controller when:
    a) data processing is performed with the consent of the Data Subject or performed by an agreement between the Company and the Data Subject;

b) Personal Data is processed by automated means;
c) the Data Subject has provided the Company with the Personal Data that he / she intends to transfer to another data controller himself / herself;
d) the Personal Data provided by the Data Subject are systematized and presented in a commonly used and computer-readable format.

2. 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 to the Data Subject, to another controller if:
   a) the Data Subject indicates in the request that the Company should transfer the Personal Data to another data controller;
   b) there are technical possibilities to provide Personal Data directly to another controller.
3. If the Data Subject 's request for transfer of Personal Data is implemented by transferring theData 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 hasa legal basis to receive the Data Subject 's Personal Data. The Company does not take responsibility for the further processing of the transferred Personal Data by another data controller.
4. 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.
5. 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 onit or to perform a task performed in the public interest.

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

1. 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:
   a) the Data Subject disputes the accuracy of his Personal Data processed by theCompany. 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;
   b) 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;
   c) 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;
   d) 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;

e) 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.

2. 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 restrict the processing of Personal Data of the Data Subject.
3. 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.

EXERCISE OF THE RIGHT TO RECTIFICATION OF THE PERSONAL DATA

1. The Data Subject shall have the right to obtain from the Company without undue delay the rectification of inaccurate Personal Data concerning him or her.
2. Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.

EXERCISE OF THE RIGHT TO WITHDRAWAL A CONSENT

1. The Data Subject has the right to withdraw consent at any time. Withdrawal of consent does not affect lawfulness of processing based on consent before its withdrawal - if processing is based on consent, including in the case of using the AIS service.
2. The Payment Service User may send a declaration of withdrawal of consent to the Company's contact address provided in these Rules.

EXCERSISE OF THE RIGHT TO OBJECT THE PROCESSING OF PERSONAL DATA

1. The Data Subject has right to provide a written notice of objection to the processing of Personal Data - if the basis for the processing of Personal Data is Art. 6(1)(f) GDPR. The objection should be justified by the particular situation of the Data Subject. Notification to the Company may be made directly, by registered mail or by electronic means.
2. 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.

CHAPTER VIII
PERSONAL DATA STORAGE PERIOD

1. Personal Data will be stored for a period depending on the purpose of processing: for the purpose of:
    a) performance by the Company of its obligations arising from the concluded contract for the

provision of Payment Services - for the duration of the contract;

b) providing the functionality of the website and maintaining the connection - for the duration of the connection;

c) fulfillment of obligations arising from legal regulations, including tax law, accounting and financial reporting regulations - we may also process data for the period necessary to fulfill the obligations specified in these regulations - for a period of 8 or 5 years;

d) determining, pursuing or defending against claims - during the limitation period for possible claims.

2. If Payment Service User has consented to the processing of Personal Data, we will process it until the consent is withdrawn or until the purpose of data processing is fully achieved (if possible) - subject to section 1 letter c above.

CHAPTER IX
THE RIGHT TO SUBMIT A COMPLAINT TO THE SUPERVISORY AUTHORITY

Data Subject also has the right to lodge a complaint with the supervisory authority responsible for the protection of Personal Data in the Member State of your habitual residence, place of work or place of the alleged infringement. In the case of Poland, this authority is:
President of the Personal Data Protection Office
Address: Stawki 2, 00-193 Warsaw
Phone: 22 531 03 00

CHAPTER X
SOURCE OF PERSONAL DATA

1. The Company obtains Personal Data of Payment Service Users from Partners. The rules for providing Personal Data are specified each time in the agreement concluded with the Partner.
2. The scope of Personal Data that is transferred to the Company is specified in these Rules.
3. Payment Service User data obtained by the Company from the Partner will be automatically completed on the Company's website through which the Company provides Payment Services.

CHAPTER XI
DATA PROTECTION IMPACT ASSESSMENT

1. When an undertaking starts new data processing operations, the Company must carry out a data protection impact assessment if the processing:

a) would seriously jeopardize the rights and freedoms of Data Subject s (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.;

b) 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);

c) large-scale processing of sensitive Personal Data.

2. If the Company, during the data protection impact assessment, determines that the rights and freedoms of Data Subject s may be seriously endangered, it must consult with the State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) on the implementation of appropriate security and other measures.
3. In performing the data protection impact assessment, the Company must determine:
   a) what data processing operations will be performed;
   b) the extent to which a specific data processing operation is necessary andproportionate;
   c) what the impact may be on Data Subjects;
   d) what are the possible measures for elimination of potential dangers, ensuring security.
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 documentedand stored.
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 theperformed cyber-attacks, intrusions into the Company's system, the data would be providedto new data recipients, processors outside the European Union, etc.
6. The data protection impact assessment may also be performed in cases not discussed in this Chapter, but upon the recommendation of the Director of the Company or the State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija).

CHAPTER XII
MANAGEMENT OF PERSONAL DATA BREACHES

1. A Personal Data breach is any intentional or negligent Personal Data breach when:
   a) Personal Data is destroyed, lost or altered;
   b) Personal Data is disclosed without permission;
   c) unauthorized persons would have access to Personal Data without permission.
2. If the violation of Personal Data security endangers the rights and freedoms of Data Subject s, the official appointed by the Director of the Company must immediately, but not later than within 72 hours, notify the State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) about the data security violation. If the Personal Data security breach is not reported to the State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) within 72 hours, the reasons for the delay must be attached to the notification.
3. In the event of a particularly serious threat to the rights and freedoms of Data Subject s, information on the breach of security must also be provided to the Data Subject s without delay. If it is not possible to inform all Data Subject s 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.
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 XIII

TECHNICAL AND ORGANIZATIONAL MEASURES FOR THE PROCESSING OF PERSONAL DATA

1. These General Requirements for Organizational and Technical Data Security Measures of the Company establish general requirements for organizational and technical data securitymeasures to protect Personal Data from accidental or unlawful destruction, alteration, disclosure, as well as from any other unlawful processing.
2. 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:
   a) 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;
   b) safe and proper organization of work and other administrative measures;
   c) practical tests are performed for disaster recovery of Personal Data;
   d) performing a data backup;
   e) 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;
   f) performing IS functionality and data integrity and readiness testing;
   g) performing a pilot data recovery.

CHAPTER XIV

PROCEDURE FOR KEEPING DATA ACTIVITY RECORDS

1. The procedure for keeping records of data activities in the Company is used in accordance with the following principles:
   a) must be used strictly for work purposes only;
   b) 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.
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 shallbe 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.
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 XV
FINAL PROVISIONS

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.
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 - GDPR), 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: Laisvės pr. 60-308 LT-05120 Vilnius.

_____ _____

(signature) *(name, surname)*