PRINCIPLES OF PERSONAL DATA PROCESSING AT FINNOVATIVE SOLUTIONS UAB

CHAPTER I GENERAL PROVISIONS

1. The Finnovative Solutions UAB Personal Data Processing Rules (hereinafter referred to as the **"Rules"**) govern the processing of personal data of individuals whose data is processed by Finnovative Solutions UAB (hereinafter referred to as the "**Company**"), establish the procedure for the exercise of their rights, organizational and technical data protection measures, procedures for managing personal data security breaches, data protection implications, personnel monitoring and functions of personal data controllers.
2. The controller of the Personal Data specified in the Rules is Finnovative Solutions UAB, legal entity code 305206391, registered address: Upės str. 23, LT-08128, Vilnius. The contact details of the Personal Data Controller are:
    a) address for written correspondence: Laisvės pr. 60-308 LT-05120 Vilnius, Republic of Lithuania
    b) e-mail address: contact@finnovative.eu
3. When processing Personal Data, the Company complies with the requirements for processing personal data as set forth in the Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter — "**ADTAĮ**"), the general requirements for organizational and technical security measures for personal data approved by the Director of the State Data Protection Inspectorate on November 12, 2008 by Order No. 1T-71 (1.12): "On approval of general requirements for organizational and technical security measures for personal data" (hereinafter: "**General Requirements**") and other legislation related to the processing and protection of personal data and the Regulation of the European Parliament and of the Council (EU) 2016/679 of April 27, 2016 on the protection of individuals 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 "GDPR").**
4. These Rules must be complied with by data processors who retrieve and process Personal Data when providing data processing services to the Company.

CHAPTER II BASIC CONCEPTS

1. **AIS —** means an online service for providing consolidated information on one or more payment accounts held by a Payment Service User with another Payment Service Provider or with more than one Payment Service Provider, provided by the Personal Data Controller.
2. **Data Subject** — means Payment Services Users, interested parties and other individuals whose data is processed by Finnovative Solutions UAB.
3. **Data Processor —** means an entity that processes Personal Data managed by Finnovative Solutions UAB in accordance with the instructions of Finnovative Solutions UAB and in accordance with the concluded service agreements.

4. **Internal administration** — means activities that ensure the independent operation of the data controller (structure management, personnel management, management and use of financial resources, clerical management).
5. **Partner** — an entity cooperating 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 customers and which makes Personal Data available to the Personal Data Controller for processing by the Personal Data Controller for the purposes indicated by the Personal Data Controller.
6. **Payment Services** — means both AIS and PIS provided by the Company.
7. **Payment Services User** — means the Partner's customer or any other person using Payment Services provided by the Personal Data Controller on the basis of a separate one-time payment services agreement concluded with the Payment Services User.
8. **Personal Data ---** means 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 / date of birth.
9. **PIS —** means the service of initiating a payment order at the request of a Payment Service User with respect to a payment account maintained by another payment service provider, provided by the Personal Data Controller.
10. **Data processing —** means an operation or sequence of operations performed in an automated or non-automated manner on Personal Data or sets of Personal Data, such as collection, recording, organizing, systematizing, storing, adapting or modifying, retrieving, sharing, using, disclosing, transferring, distributing or otherwise making available, as well as compiling or combining with other data, limiting, deleting or destroying.
11. **Personal Data Controller** — means the company Finnovative Solutions UAB, which processes the data of interested parties, other individuals, and determines the methods and means of use of such data.
12. **Data disclosure** — means disclosure of Personal Data by transferring it or making it otherwise available (excluding publication in the media).
13. Other terms used in the Principles shall be understood as defined in ADTAĮ and/or GDPR.

CHAPTER III
DATA PROCESSING RULES

1. In the course of performing independent functions, the Company's departments process Personal Data in accordance with their competencies in order to provide services, perform internal administrative functions.
2. The time limits for the storage of Personal Data and the actions to be taken after the expiration of the time limit are specified in the legal acts governing the processing of Personal Data. Personal Data is kept no longer than necessary for the purposes of processing. Specific time limits for the storage of personal documents (data) may be specified in the Rules. The data processing rules of the relevant units of the Company may be transferred to the state archives in accordance with the established procedure and provisions of Lithuanian law.

CHAPTER IV
PURPOSES OF PERSONAL DATA PROCESSING

1. The Personal Data Controller processes the Personal Data of Payment Services Users for the following purposes:
    a) In order to perform the Payment Services agreement — including the performance of obligations under the agreement, including the processing of complaints — the legal basis is the necessity of the processing to take action prior to the conclusion of the contract and in order to perform the contract (Article 6(1)(b) of the GDPR);
    b) For the purpose of transferring Personal Data to the Partner — on the basis of consent to transfer (Article 6(1)(a) of the GDPR) — when using the AIS service;
    c) For the purpose of transferring Personal Data to the Partner, which includes information about the successful initiation of a payment order, the transaction identification number, the amount of the payment transaction and, if applicable, the amount of any fees due for the transaction to the Personal Data Controller and an itemization of these amounts — based on consent for their transfer (Article 6(1)(a) of the GDPR) - when using the PIS service;
    d) In order to comply with legal obligations, including those governing the provision of Payment Services, tax law, accounting and financial reporting regulations — the legal basis is the need to comply with legal obligations (Article 6(1)(c) of the GDPR);
    e) For the purpose of establishing, investigating or defending against claims — the legal basis is the necessity of the processing for the performance of the agreement (Article 6(1)(b) of the GDPR) or the necessity of the processing to fulfill the obligations incumbent on the Personal Data Controller (Article 6(1)(c) of the GDPR);
    f) In order to pursue the legitimate interests of the Personal Data Controller, i.e. the performance of the AIS Service or the PIS Service by the Personal Data Controller (Article 6(1)(f) of the GDPR) — in the case of Personal Data of a "silent party to the transaction", i.e. entities that are not parties to the Payment Services agreement (including, but not limited to, recipients of the transaction at the PIS Service, parties to the transaction, included in the payment account information, other than the Payment Services User at the AIS Service).
2. Personal Data will not be processed by automated means, including profiling.

CHAPTER V

SCOPE OF PERSONAL DATA

1. The Personal Data Controller may process the following Personal Data of the Payment Services User during the provision of the Payment Services:in the case of performing PIS service:
    - name or company name, name of the owner or owners of the account as provided by the system of the payment account provider (e.g. bank), account number, date of posting, transaction amount, account number of the other party to the transaction, name and address of the other party to the transaction, title of the transaction, type of transaction, details of the transaction, bank details of the sender and recipient;
    - tax identification number (TIN/NIP)
    - tax data (for transactions related to the Social Security Institution or the Internal Revenue Service), such as TIN/NIP (also indicated above) or identity card number, additional payer identification number, payment type, declaration number, declaration period, payment type identifier, enforcement title number, payer identifier, payer identifier type;
    - e-mail address;

- PESEL Number
- technical data related to the device: IP address,

b. When performing AIS service:

- name or company name, name of the account owner(s) provided by the payment account provider's system (e.g. bank), account number, account balance, transaction status (executed, pending, rejected, scheduled, withheld), transaction date, posting date, transaction amount, account balance after the transaction, account number of the other party to the transaction, name and address of the other party to the transaction, transaction title, transaction type, transaction details, bank details of the sender and receiver;
- tax identification number (TIN/NIP);
- tax data (for transactions related to the Social Security Institution or the Internal Revenue Service), such as TIN/NIP (also indicated above) or identity card number, additional payer identification number, payment type, declaration number, declaration period, payment type identifier, enforcement title number, payer identifier, payer identifier type;
- PESEL No.,
- e-mail address,
- technical data related to the device: IP address.

2. The scope of the data indicated in paragraph 1 above may vary, depending on the source of the Personal Data referred to in Section X of the Rules.

CHAPTER VI
RECIPIENTS OF PERSONAL DATA

1. The Company shall share the data of Payment Services Users with data recipients only in accordance with the concluded contract or a one-time request of the data recipient, without prejudice to the requirements of legal acts and ensuring the confidentiality of personal data. In particular, in the case of the use of the AIS service, the Company may share the Personal Data of the Payment Services User with the Partner in accordance with the agreement concluded with the Payment Services User. With the consent of the Payment Services User, the Company may provide data on the status of the transaction, i.e. information on the successful initiation of the payment order, the transaction identification number, the amount of the payment transaction and, if applicable, the amount of any fees due for the transaction to the Personal Data Controller and an itemization of these amounts — in the case of the PIS Service.
2. In the case of a single transfer of data, the Company, when transferring Personal Data at the request of the data recipient, shall give priority to the transfer of data by electronic communication.
3. The Company may transfer Personal Data to entities that process Personal Data on behalf of the Company, i.e. IT and email service providers, technology providers, accountants, media destruction entities.
4. In particular, Savangard sp. z o.o., based in Warsaw, with which the Company has entered into an agreement to entrust the performance of activities within the scope of the Payment Services provided, is the entity that processes the Personal Data within the scope of the Payment Services.
5. Personal Data may also be transferred to entities entitled to request such data under applicable laws.
6. Personal Data will not be transferred to recipients outside the European Economic Area (EEA).

CHAPTER VII
DATA SUBJECTS' RIGHTS AND PROCEDURES

GENERAL PROVISIONS

Data subjects have the following rights enshrined in the GDPR:

a) the right to information (to be informed) about the processing of Personal Data in the Company;
b) the right to access your Personal Data processed by the Company;
c) the right to rectify Personal Data;
d) the right to request deletion of Personal Data (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.

THE RIGHT TO BE INFORMED ABOUT THE PROCESSING OF THE USER'S PERSONAL DATA

1. The right to information about the processing of personal data is exercised as follows:
   a) informing Data Subjects that oral consultations provided by the Company by telephone will be recorded — if the Company provides such an option;
   b) informing the Payment Services User connecting each time to the Company's electronic services management system about the processing of personal data;
   c) making information available on the Company's website,
   d) informing about the processing of Personal Data when communicating with the Data Subject in the manner in which the Data Subject addresses the Company;
   e) informing about the processing of Personal Data in other ways, taking into account the nature and specificity of the Personal Data processing operations carried out.
2. The Company shall have the right to refuse to exercise the Data Subject's right under this section of the Rules or to provide incomplete information requested by the Data Subject if:
   a) the Data Subject already has this information;
   b) providing the information requested by the Data Subject is not possible or would require a disproportionate effort;
   c) receipt or disclosure of Personal Data is expressly stipulated in legal acts of the European Union or in legal acts of the Republic of Lithuania that establish appropriate measures to protect the interests of Data Subjects;
   d) Personal Data must remain confidential, in accordance with the obligation of professional secrecy regulated by legal acts of the European Union or legal acts of the Republic of Lithuania.

EXERCISING THE RIGHT TO ACCESS OWN PERSONAL DATA

1. In accordance with the procedure established in these Rules, the Data Subject has the right to free of charge:

a) familiarize themselves with their Personal Data processed by the Company;
b) receive information from which sources and what Personal Data was collected;
c) learn for what purpose its Personal Data is processed;
d) where possible, obtain information about the expected period of storage of Personal Data or, if this is not possible, the criteria used to determine this period; the recipients or categories of recipients to whom Personal Data has been or will be disclosed, in particular recipients in third countries or international organizations;
e) be informed of the right to request the Data Controller to rectify or erase Personal Data or to restrict the processing of Personal Data concerning the Data Subject or to object to such processing;
f) obtain information about the right to file a complaint with the supervisory authority;
g) obtain information on the existence of automated decision-making, including profiling, as referred to in Article 22 (1) and (4) of the GDPR, and, at least in these cases, relevant information on the principles of such decision-making, as well as on the significance and anticipated consequences of such processing for the Data Subject.

2. If the Data Subject, after reviewing his/her Personal Data, discovers that his/her Personal Data is incorrect, inaccurate or incomplete and requests the Company to do so, the Company shall promptly, but no later than within 5 business days, verify the Personal Data and the Data Subject's written request in person, by mail or electronic means of communication, shall promptly correct the incorrect, inaccurate or incomplete Personal Data processed by the Company and (or) suspend the processing of such Personal Data, except for storage until the incorrect, inaccurate and incomplete Personal Data is corrected or the Personal Data is destroyed.
3. The Company shall promptly, but no later than within 3 working days, inform the Data Subject of the rectification, destruction or suspension of the processing activities of the Personal Data performed or not performed at the request of the Data Subject. The Company shall also promptly inform recipients of Personal Data about rectification or destruction of Personal Data at the request of the Data Subject, suspension of Personal Data processing activities, unless the provision of such information would be impossible or unreasonably difficult (due to a large number of Data Subjects, data storage period, unreasonable costs). In such case, the Company shall immediately, but no later than within 3 working days, notify the State Inspector for Personal Data Protection (Valstybinė duomenų apsaugos inspekcija).
4. A request for access to Personal Data can be made using the sample form in Appendix 1.

EXERCISING THE RIGHT TO REQUEST DELETION OF PERSONAL DATA

1. The Data Subject has the right to request erasure (right to be forgotten) of his/her Personal Data or restriction of data processing, with the exception of storage, when data is processed in violation of the requirements of legal acts. This right is exercised on one of the following grounds:
    a) Personal Data is no longer necessary for the purposes for which it was collected or otherwise processed;
    b) the Data Subject revokes the consent on which the processing was based and there is no other legal basis for the processing;
    c) Personal Data was processed illegally;
    d) Personal Data must be deleted in accordance with legal obligations under European Union

or national law.

2. The Data Subject's request must include a detailed argumentation of the reasons why he/she requests the deletion of his/her Personal Data (the request must specify one of the reasons set forth in these Rules).
3. The right to request erasure of Personal Data (right to be forgotten) is not exercised in the Company when the processing of Personal Data is necessary:
    a) in order ensure compliance with the requirements of the legal acts of the European Union and the Republic of Lithuania;
    b) for archival purposes in the public interest;
    c) to establish, assert or defend claims.
4. Upon receipt of a Data Subject's request, the Company shall promptly, but no later than within 10 business days of receipt of the request, evaluate the request to determine whether the Data Subject's request is justified.
5. If it is determined that the request made by the Data Subject is legitimate, the Company must:
    a) promptly, but no later than within 5 business days, delete all available Personal Data concerning the Data Subject;
    b) if it is not possible to immediately delete the Personal Data of the Data Subject, suspend the processing of the Personal Data of the Data Subject;
    c) inform the Data Subjects of the deleted Personal Data no later than 5 business days after the deletion of the Personal Data;
    d) inform data recipients of Personal Data deleted at the request of the Data Subject, if the Data Subject's Personal Data has been transferred to data recipients. It is not necessary to inform the recipients of the data when it is impossible or unreasonably difficult to provide such information (due to the large number of Data Subjects, the period of storage of Personal Data, unreasonably high costs).

EXERCISING THE RIGHT TO REQUEST THE TRANSFER OF PERSONAL DATA

1. The Data Subject has the right to request the Company to receive Personal Data concerning him/her and has the right to request the transfer of the Data Subject's Personal Data processed at the Company to another data controller when:
    a) processing is carried out with the consent of the Data Subject or on the basis of a contract between the Company and the Data Subject;
    b) Personal Data is processed by automated means;
    c) the Data Subject himself/herself provided the Company with the Personal Data that he/she intends to transfer to another data controller;
    d) Personal Data provided by the Data Subject is systematized and presented in a commonly used computer-readable format.
2. Upon receipt of a Data Subject's request to exercise his or her right, the Company shall promptly, but no later than 10 business days from the date of receipt of the request, evaluate the request to determine whether the request made by the Data Subject is justified. If the request is reasonable, the information may be transferred to the Data Subject and 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 transfer Personal Data directly to another controller.

3. If the Data Subject's request for the transfer of Personal Data is implemented by transferring the Data Subject's Personal Data to another data controller, the Company shall 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. The Company shall not be responsible for the further processing of the submitted Personal Data by another data controller.
4. The Company shall ensure that in exercising the right to data portability by Data Subjects, only data processed under contract or consent and processed by automated means shall be transferred. In such a case, the Personal Data will be provided to the Data Subject in a structured, commonly used computer-readable format.
5. The Data Subject's right to data portability does not apply in cases where the processing of Personal Data is necessary for the Company to fulfill a legal obligation imposed on it or to perform a task carried out in the public interest.

EXERCISING THE RIGHT TO RESTRICT THE PROCESSING OF OWN PERSONAL DATA

1. The Data Subject has the right to request the Company to restrict the processing of his/her Personal Data if one of the following grounds exists:
    a) The Data Subject questions the accuracy of his/her Personal Data processed by the Company. In such a case, the processing of the Personal Data of the data subject may be limited to the period during which the Personal Data Controller verifies the accuracy of the Personal Data;
    b) it has been determined that the processing of the Data Subject's Personal Data was unlawful, but the Data Subject does not consent to the erasure of the Personal Data, but instead requests that the processing be restricted;
    c) if the purpose of the processing of the Personal Data has been achieved and the Company, as the Personal Data Controller, no longer needs the Personal Data collected from the Data Subject to achieve that purpose, but it is needed by the Data Subject to express, enforce or assert legal claims;
    d) the Data Subject has submitted a request to the Company in which he/she expressed his/her lack of consent for the Company to process his/her Personal Data. In such a case, the processing of the Data Subject's Personal Data may be limited to the period during which the Controller verifies the legitimacy of the Data Subject's request;
    e) the Data Subject submits a request for erasure of Personal Data processed by the Company and it is determined that the request is justified, but it is not technically possible to immediately erase the Data Subject's Personal Data. In such a case, the processing of the Data Subject's Personal Data may be restricted until the Data Subject's Personal Data is deleted.
2. Upon receipt of a request from a Data Subject, the Company shall promptly, but no later than within 10 business days of receipt of the request, evaluate the request to determine whether the request made by the Data Subject is justified. If it is determined that the request made by the Data Subject is justified, the Company must restrict the processing of the Data Subject's Personal Data;
3. If 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.

EXERCISING THE RIGHT TO RECTIFY PERSONAL DATA

1. The Data Subject has the right to obtain from the Company without undue delay the rectification of inaccurate Personal Data concerning him/her.
2. Taking into account the purposes of the processing, the Data Subject has the right to complete incomplete Personal Data, including by providing an additional statement.

EXERCISING THE RIGHT TO WITHDRAW CONSENT

1. The Data Subject has the right to withdraw consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent before its withdrawal — if processing is carried out on the basis of consent, including in the case of use of the AIS service.
2. A Payment Services user may send a statement on withdrawal of consent to the Company's contact address specified in these Rules.

EXERCISING THE RIGHT TO OBJECT TO THE PROCESSING OF PERSONAL DATA

1. The Data Subject has the right to object in writing to the processing of Personal Data — if the basis for the processing of Personal Data is Article 6(1)(f) of the GDPR. 6(1)(f) of the 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 electronically.
2. If the request is unreasonable, the Company shall indicate to the Data Subject in writing the reasons why the Data Subject's Personal Data must continue to be processed for legitimate and lawful reasons that outweigh the Data Subject's interests;

CHAPTER VIII
RETENTION PERIOD OF PERSONAL DATA

1. Personal Data will be kept for a period depending on the purpose of processing:
    a) for the performance by the Company of its obligations under the Payment Services Agreement — for the duration of the agreement;
    b) to ensure the functionality of the website and maintain the connection — for the duration of the connection;
    c) for the fulfillment of legal obligations, including the Lithuanian law on payment services, taxation, accounting and financial reporting regulations — we may also process the data for the period necessary to fulfill the obligations set forth in these regulations, not longer than 8 years;
    d) to establish, assert or defend against claims — during the period of limitation of possible claims.
2. If a Payment Services User has consented to the processing of Personal Data, we will process the Personal Data until the withdrawal of his/her consent or until the purpose of the processing is fully achieved (if possible) — subject to paragraph 1(c) above.
3. After the expiration of the periods indicated above, the Personal Data will be deleted or anonymized. The Personal Data Controller will exercise due diligence, in order to process the Personal Data in the

shortest possible time.

CHAPTER IX
THE RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY

The Data Subject also has the right to lodge a complaint with the supervisory authority responsible for data protection in the Member State of his or her habitual residence, his or her place of work, or the place where the alleged violation was committed. In the case of Poland, this body is:
President of the Office for Personal Data Protection
Address: Stawki 2, 00-193 Warsaw
Phone no.: 22 531 03 00

CHAPTER X
SOURCE OF PERSONAL DATA

1. The Company obtains Personal Data of Payment Services Users from Partners. The terms of transfer of Personal Data are defined in each case by the agreement concluded with the Partner.
2. The Company obtains Personal Data from Payment Service Providers of Payment Service Users who maintain payment accounts (banks), who provide Personal Data of Payment Service Users to the Company in accordance with the internal regulations of the respective account provider.
3. The scope of Personal Data provided to the Company is set forth in these Rules. It may vary depending on the internal regulations of the Payment Service User's payment service provider.
4. The Payment Services 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 the Company begins new data processing operations, it must conduct a data protection impact assessment if the processing:
   a) would seriously jeopardize the rights and freedoms of Data Subjects (for example, transfer of data outside the European Union or processing of data obtained by combining data from other sources, introduction of new technological solutions such as facial recognition systems), etc;
   b) for automated processing of Personal Data, profiling and legal or other decisions with significant consequences (for example, where processing may lead to exclusion or discrimination of individuals);
   c) for large-scale processing of sensitive Personal Data.
2. If the Company determines during a data protection impact assessment that the rights and freedoms of Data Subjects may be seriously threatened, it must consult with the State Data Protection Inspector (Valstybinė duomenų apsaugos inspekcija) on the implementation of appropriate security and other measures.
3. In assessing the impact on data protection, the Company must determine:
   a) what data processing operations will be performed;

b) the extent to which a particular data processing operation is necessary and proportionate;
c) what impact this may have on Data Subjects;
d) what are the possible measures to eliminate potential risks, ensuring safety.

4. The Company must ensure that the data protection impact assessment described in this chapter and conducted by the Company in the cases provided for is properly documented and retained.
5. Data protection impact assessments may also be conducted for existing data processing operations if there are significant changes to these operations, such as the introduction of new technologies, processing of data for a different purpose, new risks associated with cyber-attacks carried out, intrusions into the Company's system, data will be transferred to new data recipients, processors outside the European Union, etc.
6. A data protection impact assessment may also be conducted in cases not discussed in this chapter, but on the recommendation of the Company Director or the State Data Protection Inspector (Valstybinė duomenų apsaugos inspekcija).

CHAPTER XII
MANAGING PERSONAL DATA BREACHES

1. A Personal Data breach is any intentional or negligent violation of Personal Data protection when:
   a) Personal Information is destroyed, lost or altered;
   b) Personal Information is disclosed without authorization;
   c) unauthorized persons would have access to Personal Data without permission.
2. If a security breach of Personal Data threatens the rights and freedoms of Data Subjects, an employee designated by the Company Director must notify the State Data Protection Inspectorate (Valstybinė duomenų apsaugos inspekcija) of the data security breach immediately, but no later than within 72 hours. If a 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 report.
3. In the case of a particularly serious threat to the rights and freedoms of Data Subjects, information about the security breach should also be immediately communicated to Data Subjects. If it is not possible to inform all Data Subjects due to the large number of Data Subjects or for other reasons, an employee of the Company, together with the Company Director, shall consider and decide whether to provide this information through the media.
4. In the event of a breach of Personal Data referred to in this section of the Rules, a Company employee shall, in addition to other duties discussed in this section, prepare an action plan containing preventive measures to prevent similar data breaches in the future and submit it to the Company Director.

CHAPTER XIII
TECHNICAL AND ORGANIZATIONAL MEANS OF PERSONAL DATA PROCESSING

1. These general requirements for organizational and technical data security measures of the Company set forth the 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.

2. The following infrastructure, administrative and telecommunications (electronic) measures are in place to protect Personal Data from accidental or unlawful destruction, alteration, disclosure or any other unlawful processing:
   a) safe and proper deployment and maintenance of equipment, maintenance of information systems (IS), network management (LAN, wireless), security of Internet use and other information technology measures;
   b) safe and proper organization of work and other administrative measures;
   c) practical tests of disaster recovery of personal data are carried out;
   d) performing data backup;
   e) provision of data recovery from the latest available backup in the event of data loss due to hardware failure, software error or other breach of data integrity;
   f) conducting tests of IS functionality and data integrity and readiness;
   g) performing pilot data recovery;

CHAPTER XIV
PROCEDURE FOR KEEPING RECORDS OF DATA ACTIVITY

1. The Company's data activity record-keeping procedure is applied in accordance with the following:
   a) it must be used exclusively for business purposes;
   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 will be reviewed at least once a year, and if necessary or in the case of a change, the documents governing the processing of Personal Data will be updated by implementing structural, technological or other changes. An employee of the Company is responsible for supervising compliance with the provisions of this Procedure and controlling the implementation of the provisions regulated herein, as well as initiating its renewal when necessary.
3. Any activities not provided for in this chapter related to the keeping of data records of the Company's activities must be coordinated with an employee of the Company.

CHAPTER XV
FINAL PROVISIONS

1. The Rules will be reviewed at least once every 2 years, and if necessary or in the case of a change, the legal acts governing the processing of Personal Data will be updated. Compliance with the provisions of these Rules will be monitored and updated as necessary by an officer of the Company.
2. The actions and decisions of the implementing entities of the Principles may be appealed in accordance with the procedures set forth in legal acts.

Principles of personal data processing
Appendix no. 1

(Personal data request form)

To the director of Finnovative
Solutions UAB

PERSONAL DATA ACCESS REQUEST

_____
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 — Company) holds about you. Information on how the company processes your Personal Data will be provided 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 correctly identify: you as a Data Subject; and your information. To help us effectively respond to your inquiry, please provide the company with the following information in writing. You can fill out this form and send it back to us:

No.	**Description**	**To be completed by the applicant**
January	Name, surname (required)	
2.	address	
3.	e-mail address	
4.		

In order to expedite our search, please provide as much data as possible about the requested information and, if possible, where it is 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 have.
I certify that all Personal Information requested has been provided. Please send the completed and signed form by email or snail mail to the address below: Upės g. 23, LT-08128 Vilnius.

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