1. Purpose and application of the privacy statement

1.1. The privacy statement (hereinafter also referred to as - the Statement) is developed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter - the Regulation).

1.2. The purpose of this Statement is to provide information to the personal data subject - identifiable natural persons (hereinafter - the Data Subject or you) on how the controller of personal data processing - JSC VIRŠI-A (hereinafter - the Controller or VIRŠI) collects, processes, stores, shares, deletes and protects the personal data. The purpose of the Statement is to protect the interests and freedoms of the Data Subject, at the same time ensuring that personal data are processed lawfully, in good faith and in a manner that is transparent to the Data Subject.

1.3. For the specific processing of personal data, the Controller has developed separate privacy statements, about which the Controller also provides information in this Statement. Taking the above-mentioned into account, this Statement shall be deemed a general privacy statement, and privacy statements developed for the specific processing of personal data constitute a special privacy statement. In the case of conflict, the terms and conditions of the special privacy statements shall prevail.

1.4. This statement shall apply to the processing of personal data of natural persons, regardless of the form and/or environment in which the natural person provides the personal data (during face-to-face contact, orally in writing, by post, telephone, electronic or other technical means of communication, including mass media and on the application etc.), as well as regardless of the source of acquisition of personal data and the systems in which the data is processed.

2. Personal data controller and contact details

2.1. The controller of personal data processing specified in this Statement shall be **JSC VIRŠI-A** (unified registration No. 40003242737), whose contact information is as follows:

- legal address: Kalna iela 17, Aizkraukle, Aizkraukle Rural Territory, Aizkraukle Municipality, LV-5101, Latvia;
- e-mail address: birojs@virsi.lv;
- telephone 80 700 070.

2.2. You can contact the Data Protection Officer of VIRŠI about all personal data processing and protection issues in the following ways:

- E-mail address: datuaizsardziba@virsi.lv;
- address for correspondence: Kalna iela 17, Aizkraukle, Aizkraukle Rural Territory, Aizkraukle Municipality, LV-5101, Latvia.

Address the letter to: Data Protection Officer of AS Virši-A.

2.3. The controller of personal data processing determines what personal data are collected and

for what purposes, as well as the way they are processed.

3. How will you be informed about the processing of your personal data?

3.1. In order to facilitate the processing of transparent data, the Controller shall inform and explain what personal data are processed in the course of the commercial activity of the Controller and how they are used. The above-mentioned information is provided in this Statement.

3.2. When processing personal data for purposes not specified in this Statement, as well as to clarify information about the individual conditions of data processing, the Controller may inform you separately (for example, by placing notices in the e-mails). Besides, the information may also be provided to you by personnel of the Controller, explaining it orally or asking to become acquainted with the information specified in certain documents.

4. What are the applicable legal acts?

4.1. Collection and processing of personal data is performed in accordance with the following regulatory enactments:

4.1.1. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

4.1.2. Personal Data Processing Law (*Fizisko personu datu apstrādes likums*);

4.1.3. other regulatory enactments binding to the Controller, which are applicable in relation to the processing and protection of personal data, for example, the Law On Accounting or the Law On Prevention of Money Laundering and Terrorism and Proliferation Financing.

5. What is personal data?

5.1. Personal data means any information related to an identified or identifiable natural person ("Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the natural person.

6. What are the purposes of personal data processing?

In the course of commercial activity, the Controller has determined that it shall have the following purposes for the processing of personal data:

6.1 Processing of personal data for ensuring the economic activity of the Controller, concluding contracts and fulfilling contractual obligations and ensuring the legitimate interests of the Controller.

6.1.1. What personal data are processed by the Controller?

The categories of personal data processed by the Controller depend on the specific situation in which the personal data is processed, i.e., the economic activities performed by the Controller, the

requirements of regulatory enactments and the legitimate interests of the Controller in the specific situation.

For example, when the Data Subject expresses (by telephone, e-mail, website www.virsi.lv , etc.) a wish to enter into an agreement (for example, a fuel card agreement) or by asking about the agreement that has already been concluded between the Parties. In this case, the Controller shall be obliged to process information that proves your identity (for example, name, surname, personal identity number, delivery address, available fuel quota, contact information for communication, represented company, if any, etc.). After the conclusion of the agreement, your personal data is processed in accordance with the agreement concluded between the parties, as well as payment information arising from this agreement (if the service is provided for a fee), including bank account, information about the credit institution, payments made, purchases/goods received, information about received fuel cards, granted and spent credit limit, information specified by you on the fuel card, e-mail for receiving invoices, customer number. In order to be able to follow the fulfilment of the contractual obligations, you have the opportunity to join the VIRŠI Info system, which is available on the website www.virsi.lv , indicating your personal data as a contact person (for example, name, surname, telephone and/or e-mail).

6.1.2. What is the legal basis for personal data processing?

Data processing is performed with a purpose to ensure commercial activity of the Controller, including, in order to enter and fulfil the agreement, on the basis of Article 6(1)(b) of the Regulation, that is, processing is required for fulfilment of the agreement, where the data subject is the contracting party, or the performance of measures pursuant to the request of the data subject prior to entering into the agreement.

In cases when a contractual relationship has been established between the parties, the Controller may, in accordance with the Law On Accounting, apply Article 6(1)(c) of the Regulation - processing is necessary to fulfil a legal obligation applicable to the Controller.

In all cases the Controller shall apply Article 6(1)(f) of the Regulation - processing is necessary to pursue the legitimate interests of the Company or a third party (except for if the interests or fundamental rights and freedoms of the Data subject which require the protection of personal data are more important than those interests, in particular where the data subject is a child).

The Controller shall also apply Article 6(1)(f) of the Regulation to provide evidence of the conditions for communication both before the conclusion of the agreement as well as during the fulfilment of the contractual obligations. For example, to organise the economic activity of the Controller and the fulfilment of the contract concluded with you by contacting you and/or state and/or municipal authorities, investigate cases of complaints about the quality of services/goods, carry out follow-up to improve the provision of services, as well as to provide evidence in the event of complaints, claims and litigation.

6.1.3 What is the period for personal data processing?

Upon providing the services, the Controller complies with the special laws and regulations governing its obligation to retain certain data. For example, the Law On Accounting imposes an obligation to keep information on transactions for five years. In compliance with the above-mentioned, the Controller shall observe the terms specified in regulatory enactments. In turn, when providing services and selling goods, the information shall be stored for the entire period of providing the service and selling the goods, in compliance with the requirements on limitation periods applicable to the

relevant legal relationship (for example, 3 years for commercial transactions, because one of the parties is a merchant).

At the end of the storage period, personal data will be permanently deleted, unless claims for mutual cooperation are received. In such a case, the Controller may, on the basis of his or her legitimate interest, store all or part of the information until the final settlement of the claim (i.e., the ten-year limitation period stipulated in the Civil Law or the date of entry into force of the court decision).

6.1.4 Who can access the information and to whom is it disclosed?

Recipients of personal data may be employees authorised by the Controller, in accordance with the scope specified in their work duties and in compliance with the requirements specified in regulatory enactments.

Personal data may be transferred to the processors of the Controller, such as suppliers of goods, debt collectors, legal services providers, franchisees, financial advisers, audit service providers and other consultants, in accordance with the terms and conditions of the agreement between the parties.

Personal data may be transferred to the related companies of the Controller (subsidiaries) in compliance with the requirements specified in regulatory enactments.

Personal data may be transferred to law enforcement authorities, courts or other state and local government institutions if the relevant institutions have the right to the requested information (for example, the State Revenue Service about you as a business partner, the Rural Support Service, etc.).

In order to protect the legitimate interests of the Controller, personal data may be transferred to a court or other state institution against a person who has infringed the legitimate interests of the Controller. For example, in cases where there is a dispute about the quality of oil products sold by the Controller and the inspection is performed by an independent laboratory - data on the customer involved in the particular dispute may be transferred.

Personal data shall not be transferred to recipients outside the European Union or the European Economic Area.

The Controller has a duty to provide information on the personal data processed:

1. to law enforcement institutions, the court, state and other local government institutions if it arises from laws and regulations and the institutions concerned are entitled to the information request.

2. If personal data must be transferred to a third party within the framework of a concluded contract in order to perform any function necessary for the performance of the contract (for example, in the case of a guarantee, an insurance contract; realisation of the Controller's legitimate interests, provision of legal aid).

3. According to a clear and unambiguous request of the Data Subject.

4. In order to protect the legitimate interests of the Controller, for example, when turning to a court or other state institution against a person who has infringed the legitimate interests of the Controller.

6.2. Preservation and records of incoming and outgoing communications (emails, letters by mail) to ensure the fulfilment of contractual obligations, fulfilment of duties subject to the Controller and respecting the legitimate interests of the Controller.

6.2.1. What personal data are processed by the Controller?

When contacting the Controller or submitting a complaint or suggestion by using the contact information provided by the Controller (such as telephone, e-mail, post, etc.), written information related to the specific document and the information contained therein, as well as the content of the communication, time and information about the communication tool used will be maintained. In the case that you make a claim regarding the fulfilment of the contractual obligations, the Controller will need to identify the complainant or the person who needs to prepare a reply. In this case, in order to achieve the purpose, the Controller may process the amount of personal data, which includes the name of the Data Subject, personal identity number, contact information, information on received services/purchases, personal online identification data, including information related to the history of use of services/purchases (analysis of system audit records, payment discipline (type and terms of payment, late payments), credit history, information about your debt liabilities in the available registers of debtors, etc.) and other information related to the contract. Such information is recorded in the documentation and stored in the Controller's data processing systems. The Controller has the obligation and right to process the information identifying the Data subject and information confirming the identity of the person, as well as the right of representation (if the person represents another person) in the contractual relationship.

6.2.2. What is the legal basis for personal data processing?

The maintenance of information on the fact and content of communication is carried out on the basis of Article 6(1)(f) of the Regulation - processing is necessary for the protection of the legitimate interests of the controller or of a third party, unless the interests or fundamental rights and freedoms of the data subject, which require the protection of personal data, outweigh such interests. In cases when you have submitted a document containing a request, complaint, proposal or issue which gives a rise to the Controller's obligation to examine your application, the legal basis for data processing is this legal obligation (for example, compliance with requirements of consumer protection regulatory enactments or the Regulation, as well as other regulatory enactments that regulate the settlement of the issue referred to in the submission (proposal, complaint), in accordance with Article 6(1)(c) of the Regulation - processing is necessary to fulfil a legal obligation applicable to the Controller. In turn, in order to ensure the legitimate interests of the Controller and third parties (for example, to investigate cases where complaints have been received about the quality of service provision, as well as to provide evidence against possible complaints), the legal basis of data processing shall be the legitimate interest of the Controller. Besides, recording of correspondence is performed in order to systematise the commercial activity of the Controller and achieve the goals of the commercial activity - to provide information about the range of services, conditions for purchasing goods, etc.

6.2.3. What is the period for personal data processing?

To achieve this, the Controller shall keep the information for a maximum of five years, unless the relevant information needs to be used to ensure that the Controller's legal interests are safeguarded for a longer period (for example, in the event of a dispute - for the preservation of evidence). In this

case, the information shall be stored for as long as the legal interests of the Controller or a third party exist.

If adjustments have been made to the accounting system in relation to the correspondence received, then the relevant information is stored in accordance with the regulatory enactments regulating accounting, i.e., for 5 years.

At the end of the storage period, personal data shall be permanently deleted.

6.2.4. Who can access the information and to whom is it disclosed?

Recipients of personal data may be employees authorised by the Controller, in accordance with the scope specified in their work duties and in compliance with the requirements specified in regulatory enactments, as well as providers of legal services, law enforcement, controlling, supervising and supervising institutions.

Personal data shall not be transferred to recipients outside the European Union or the European Economic Area.

6.3. Processing of personal data for the presentation of corporate information in the media, on the website administered by the Controller and on social networks for the purpose of popularising and promoting the brand name "VIRŠI".

6.3.1. What personal data are processed by the Controller?

Informative materials of the Controller, events, news, photos of persons, video and audio recordings, events organised by the Controller and information about the Controller's participation in events organised by cooperation partners can be placed in various media, Controller's website www.virsi.lv, Controller's social network platforms (such as facebook.com, instagram.com, youtube.com) and stored in the Controller's archive to promote the Controller's brand. In certain cases, these materials may also contain personal data of visitors to events organised by the Controller - photographs, video materials, audio materials, descriptions of events, information and data provided during the interview, etc.

6.3.2. What is the legal basis for personal data processing?

Personal data processing is performed on the basis of Article 6(1)(f) of the Regulation - the processing is necessary for compliance with the legitimate interests of the controller or a third person, except for if the interests or fundamental rights and fundamental freedoms of the data subject, which require the protection of personal data, outweigh such interests. This means that the Controller has a legitimate interest to present its events or events where it participates, in the media and on the Manager's website: www.virsi.lv and on social networking platforms (such as facebook.com, instagram.com, youtube.com), thus ensuring the visibility of the Controller's brand "VIRŠI".

When choosing what information to publish on the media, on the Controller's website and on social networking platforms, the Controller always tries to ensure that your rights and freedoms as a Data Subject are not violated. The Controller respects the individual's right to privacy. The Controller is aware that it does not know all the facts and circumstances about the possible impact of these activities, so in order to ensure fair processing, any person has the opportunity to contact the Controller and the right to object to the presentation of their personal data on the Controller's website or the

above-mentioned social networking platforms. In this case, the Controller shall provide information on this to the e-mail address provided in this Statement.

6.3.3. What is the period for personal data processing?

Personal data shall be stored until the purpose is achieved, i.e., for as long as the information, published for the purpose of promoting the Controller's visibility, is up-to-date, except for the information that is stored in the Controller's archive permanently. The Controller shall periodically review the information published to ensure that information which does not fulfil the purpose for which the personal data are processed is regularly deleted, except for processing for archival purposes.

6.3.4. Who can access the information and to whom is it disclosed?

Recipients of personal data may be authorised employees of the Controller, users and processors of the relevant media, the Controller's website www.virsi.lv and/or social networking platforms (such as facebook.com, instagram.com, youtube.com), law enforcement and supervisory authorities. The data may also be transferred for the fulfilment of a contract concluded between the Controller and a third party (for example, to a service provider in order to perform photo and/or video, audio, production works, website administration works, brand awareness promotion works, etc.).

The Controller informs that in order to achieve the purpose of data processing, personal data shall be processed in an electronic environment on social networking platforms administered by the Controller (facebook.com, instagram.com, youtube.com, etc.) and the processors chosen by it (facebook.com, instagram. com, youtube.com, etc.) are companies operating outside the European Union and the European Economic Area, so the Controller encourages you to read the privacy policies of these companies (for example, facebook.com privacy policy: https://www.facebook.com/privacy/explanation, instagram.com privātuma politiku: https://help.instagram.com/519522125107875), or contact the Controller with a request to provide additional information on the provisions of cooperation.

Besides, in order to comply with the principle of data processing in good faith, the Controller explains that, taking this circumstance into account, the purpose of such data processing is to publish information about the Controller's activities, and the resulting materials will be publicly available and accessible to any third party.

6.4. Personal data processing for the prevention of money laundering and terrorism financing (AML)

6.4.1. What personal data are processed by the Controller?

In order to prevent money laundering and activities related to the financing of terrorism and proliferation, the Controller processes your personal data, such as name, surname, personal identity number, address of the declared place of residence, place of commercial activity, your contact details (telephone number, e-mail), information on the material circumstances of your commercial activity (for example, on the sources of funding and their supporting documents), the details of the beneficial owners. The Controller may also retain information about you as the beneficial owner, as well as other circumstances that are relevant to the Controller to ensure that the money or other resources of you or the company, where you are the beneficial owner, are legal. The Controller, when entering into a business relationship with you or your company, where you are the beneficial owner or a

representative of the company, monitors the transactions during the transaction, including checks that the transactions entered into during the business relationship are carried out in accordance with the information about you as a customer available at the disposal of the subject of law, your commercial activity, risk profile and the origin of funds. Refusal to provide the information herein will serve as a basis to refuse to have transactions with you as a customer or company that you represent or where you are a beneficial owner.

6.4.2. What is the legal basis for personal data processing?

The personal data processing is carried out on the basis of Article 6(1)(c) of the Regulation - the processing is necessary to fulfil a legal obligation subject to the Controller, because the Controller has an obligation to obtain information about its customers, monitor customer transactions and, if necessary, to provide the available information and documents regarding each suspicious transaction to the Financial Intelligence Service and the State Revenue Service. The above-mentioned arises from the provisions of Section 3.1 of the Law of the Republic of Latvia on the Prevention of Money Laundering and Terrorism and Proliferation Financing. The Controller is obliged to report to the State Revenue Service on suspicious tax transactions performed by residents of the Republic of Latvia as required by the Law on Taxes and Duties.

Such processing shall be carried out by the Controller on the basis of Article 6(1)(f) of the Regulation - the processing is necessary for the protection of the legitimate interests of the controller or of a third party, unless the interests or fundamental rights and freedoms of the data subject, which require the protection of personal data, outweigh such interests, i.e., the Controller has a legitimate interest to perform personal data processing in order to achieve the purpose specified in regulatory enactments and to ensure that the Controller only performs transactions with cooperation partners, the source of funds of which is not in doubt.

6.4.3. What is the period for personal data processing?

The Controller will store, regularly evaluate and update the documents and information obtained in the course of due diligence of you as a customer or customer's representative (beneficial owner) in accordance with the inherent risks, but at least once every five years. The above-mentioned is determined by Section 11.1, Paragraph one, Clause 5, and Section 37, Paragraph two of the Law on the Prevention of Money Laundering and Terrorist and Proliferation Financing, which stipulates that for five years after the termination of a business relationship or execution of an occasional transaction, the Controller shall store the following:

1) all information obtained during the course of customer due diligence, including information regarding domestic and international transactions of the customer, domestic and international occasional transactions and such accounts, copies of documents certifying the customer identification data, the results of the customer due diligence, as well as the available information which has been obtained, using means of electronic identification, certification services within the meaning of Section 1, Clause 10 of the Electronic Documents Law in accordance with Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, or other technological solutions in the amount and in accordance with the procedures stipulated by the Cabinet;

2) information regarding all the payments made by the customer;

3) correspondence with the customer, including electronic correspondence.

Upon the expiry of the term for storage of the documents and information specified above, the

Controller shall destroy the documents and information regarding the person at its disposal.

6.4.4. Who can access the information and to whom is it disclosed?

Recipients of personal data may be employees authorised by the Controller, in accordance with the scope specified in their work duties, as well as providers of legal services, law enforcement, controlling and supervising institutions for the performance of functions stipulated by law.

Personal data shall not be transferred to recipients outside the European Union or the European Economic Area.

The Controller can submit your personal data:

1) supervisory and control institutions, law enforcement institutions, a court or other state (for example, the Financial Intelligence Service, the State Revenue Service and the Consumer Rights Protection Centre, etc.) institutions, if this follows from regulatory enactments and the relevant institutions have the right to the required information;

2) if the personal data shall be transferred to the relevant third party within the framework of the concluded agreement (for example, for the realisation of the legitimate interests of the Controller, for the provision of legal aid);

3) in order to protect the legitimate interests of the Controller, for example, when turning to a court or other state institution against a person who has infringed the legitimate interests of the Controller.

The Data Controller shall not provide the Data Subject with information on the processing of personal data performed within the framework of prevention of money laundering and terrorist and proliferation financing carried out within the framework of the Law on the Prevention of Money Laundering and Terrorist and Proliferation Financing, except for publicly available data**.**

6.5. Personal data processing for the purpose of administration of the lists of holders of internal information and persons closely associated with the controller and the controllers.

6.5.1. What data are processed by the Controller?

In order to ensure compliance with the requirements of Regulation (EU) No. 596/2014 of the European Parliament and of the Council on Market Abuse (hereinafter - the Market Abuse Regulation) and arising from legislation based on it, the Controller is required to establish a list of holders of internal information as well as lists of controllers and persons closely associated with it. For the purposes of the Market Abuse Regulation, a holder of internal information is a person who is a member of the Controller's administrative, management or supervisory body, a member of the Controller, and has access to the internal information if it is performing work, professional or official duties. In any case, any person who has access to the Controller's internal information may be recognised as the holder of the internal information (if he knew or should have known this fact in the specific situation).

On the other hand, a person who is a member of the administrative, management and supervisory body of the Controller or any other senior manager who regularly has access to internal information directly or indirectly related to the Controller and who is entitled to make the management decisions that affect the future development of the Controller and the prospects for concluding transactions. Besides, according to the Market Abuse Regulation, a person closely related to a person performing management duties is a person who is the spouse or equivalent partner of the person performing management duties, according to the Latvian law, a dependent child, according to the Latvian law, another relative, which has had a joint household for at least one year, as well as any other

legal person which is directly or indirectly controlled by or for the benefit of such a person, or whose economic interests are substantially equivalent to those of such a person.

In order to comply with the obligations set out in the Market Abuse Regulation, and if you are to be recognised as a holder of the internal information or a closely related person, the Controller will collect and maintain a list of the following information: Your name, date of birth, personal identity number, information about your surname at the time of birth, contact information, information about why you are on any of the lists, information about your reported transactions if you are, for example, a closely related person, information about the time and date when you are listed or deleted.

6.5.2. What is the legal basis for personal data processing?

Your personal data will be processed on the basis of Article 6(1)(c) of the Regulation in order to ensure compliance with the requirements of Regulation (EU) No. 596/2014 of the European Parliament and of the Council on market abuse, as well as our legitimate interests based on Article 6(1)(f) of the Regulation, namely to provide evidence that the requirements of the Market Abuse Regulation have been met, as well as in a situation where you do not comply or there are reasonable suspicions that you have not complied with your obligations as a holder of the internal information, a person performing management duties or a person closely associated with such a person - the relevant information may be used to prove a breach.

6.5.3. What is the period for personal data processing?

To achieve the purpose, the Controller shall store the information in accordance with the provisions of Article 18(5) of the Market Abuse Regulation, i.e., the list of information holders shall be stored for at least five years after its preparation or updating. The same condition, based on the legitimate interests of the Controller, shall apply to the lists of closely related persons and reports received. The above-mentioned five-year period may be extended if the relevant information needs to be used to safeguard the Controller's legal interests for a longer period (for example, in the event of a dispute - for the preservation of evidence). In such case, the information will be stored for as long as the legal interests of the Controller or a third party exist, i.e., until the final settlement of the dispute and the expiry of the limitation period. At the end of the storage period, personal data shall be permanently deleted.

6.5.4. Who can access the information and to whom is it disclosed?

Your personal data will be received by the investigating competent authorities, who need to both quickly analyse the behaviour of the holder of the internal information in trade as well as establish the links between the listed persons and the persons involved in the suspicious transactions and the contacts that have taken place between them at certain times. Besides, the Controller shall ensure that your personal data is only received by authorised employees and service providers and, if necessary, to submit it to law enforcement and control institutions, such as the State Police, the Prosecutor's Office, the court.

The Controller shall not plan to transfer the personal data to recipients outside the European Union or the European Economic Area.

The Controller will most likely transfer the information to the competent authority, which may in turn transfer it to the European Securities and Markets Authority, where these authorities will be recognised as separate controllers.

7. Rights of the data subject with regard to personal data processing

7.1. How is the Data Subject informed of his/her personal data processing?

The Data Subject shall be informed of the personal data processing specified in this Policy by using a multi-level approach, including such methods as placing of this Statement or a part thereof on the website of the Controller www.virsi.lv, as well as in certain cases the information will be provided in the form of statements or otherwise.

7.2. Right to access the personal data and modify them.

7.2.1. In accordance with the provisions of the Regulation, the Data Subject has the right to request access to and receive information about the Data Subject's personal data held by the Controller and to receive information on:

- what personal data about him/her is at the disposal of the Controller;
- what purposes the Controller processes this personal data;
- categories of recipients of personal data (persons to whom personal data have been disclosed or to whom they are intended to be disclosed, unless the regulatory enactments allow the Controller to provide such information in a certain case);
- information on the period for which the personal data will be stored or the criteria used to determine that period.

7.2.2. If the Data Subject considers that the information at the disposal of the Controller is out-of-date, incorrect or wrong, the Data Subject has the right to request the correction of his or her personal data.

7.2.3. The Data Subject has the right to request the deletion of his or her personal data, or to object to the processing thereof, if the person considers that data have been processed illegally, or they are not necessary anymore in relation to the purposes for which they have been collected and/or processed (upon implementing the right of principles “right to be forgotten”).

7.2.4. The Controller informs that personal data of the Data Subject cannot be deleted, if personal data processing is necessary in the following cases:

- for the Controller to protect the essentially important interests of the Data Subject or other individual, including the life and health thereof;
- in order for the Controller or any third person to establish, implement or protect lawful (legal) interests;
- data processing is required in accordance with the regulatory enactments binding to the Controller.

7.2.5. The Data Subject has the right to request that the Controller restricts the processing of personal data of the Data Subject if any of the following circumstances exist:

- accuracy of the personal data is contested by the Data Subject - for a period enabling the Controller to verify the accuracy of personal data;
- the processing is unlawful, and the Data Subject objects to the erasure of the personal data and requests the restriction of their use instead;
- the Controller does not need personal data for processing anymore, however they are

necessary for the Data Subject in order to bring, exercise or defend lawful claims;

- the Data Subject has objected to processing - while it is not verified whether legitimate reasons of the Controller are more important than the legitimate reasons of the Data Subject.

7.2.6. If the processing of personal data of the Data Subject is restricted in accordance with Paragraph 6.5, such personal data shall only be processed with the consent of the Data Subject (except for storage) or in order to bring an action, exercise or defend lawful rights, or in order to protect the rights of another individual or legal entity, or important public interests.

7.2.7. Before revocation of the restriction of personal data processing of the Data Subject, the Controller shall inform the Data Subject.

7.2.8. The Data Subject has the right to file a complaint with the Data State Inspectorate if the Data Subject believes that the Controller has processed personal data unlawfully. The Controller first invites to contact it by writing to the e-mail address: datuaizsardziba@virsi.lv in order to promptly find a solution to the situation if the Data Subject's right to personal data protection has been violated.

7.3. Right to withdraw consent.

If the Controller processes personal data on the basis of the Data Subject's consent, the Data Subject has the right to withdraw the consent at any time by sending a revocation in accordance with the procedure specified in Paragraph 2 of the Statement. Upon receipt of the revocation, the Controller will not further process the Data Subject's data for the purpose for which the consent was revoked. Besides, in order to ensure fair processing on the part of the Controller, the Controller shall, taking the technological possibilities into account, offer an additional opportunity to refuse to receive further information each time you contact us.

8. Acceptance and review of Data Subject's submissions, requests and complaints

8.1. If the Data Subject has any questions, requests, objections or complaints related to the processing of personal data performed by the Controller, the Data Subject may submit a request to the Controller regarding the exercise of his/her rights through the following communication channels:

8.1.1. by personally identifying himself/herself and presenting a personal identity document (for example, a passport or ID card, etc.) to submit a written application, request or complaint to the Controller at the contact information address specified in Chapter 2 of the Statement;

8.1.2. by sending a submission, request or complaint by post to the contact address of the Controller specified in this Statement. A reply will be drawn up and sent by using a registered letter, thus ensuring that unauthorised persons may not receive such consignment. Concurrently, the Controller shall reserve the right to request additional information from the Data Subject in the event of doubt, if the Controller considers it necessary;

8.1.3. by sending the application, request or complaint electronically to the e-mail address : datuaizsardziba@virsi.lv, signing it with a secure electronic signature. In such a case it is presumed that the Data Subject has identified himself or herself by submitting a request, which is signed with a secure electronic signature. At the same time, the Controller shall reserve the right in the case of doubts to request additional information from the Data Subject, if it considers it necessary. Electronically submitted submissions of the Data Subject shall be sent to the e-mail address: datuaizsardziba@virsi.lv;

8.1.4. In other cases, when the Controller has no doubts about the identity of the Data Subject, coordinating the procedure for issuing information.
The Controller will review a submission, request or complaint of the Data Subject and a reply will be

drawn up and sent by using a registered letter, thus ensuring that unauthorised persons may not receive such consignment. Concurrently, the Controller shall reserve the right to request additional information from the Data Subject in the event of doubt, if the Controller considers it necessary.

8.2. The Data Subject is obliged to clarify in his or her request as much as possible, the time, place and other circumstances that could help to execute his or her request.

8.3. After the receipt of a written request of the Data Subject regarding exercising his or her rights, the Controller shall:

8.3.1 verify the identity of a person;

8.3.2. assess the request and proceed as follows:

- if the Controller can ensure the execution of the request, it shall execute it as soon as possible and the Data Subject as the submitter of the request may receive the information or a copy of the data referred to in the request;

- if the Controller needs additional information to identify the Data Subject requesting the information or to fulfil the request, the Controller may request the Data Subject to provide additional information (for example, specific date or time, use of services, card data, purchase data, etc., where the Data Subject is identifiable);

- if the information is deleted or the person who requests the information is not the Data Subject or the person may not be identified, the request may be rejected in accordance with this Statement and/or regulatory enactments;

- in the case that the Controller has received the request, but the Data Subject has not left his/her contact information so that the Controller can contact it during the processing of the request and inform it about the result of the review of the Request, the Controller shall undertake to prepare a written response within one month, which will be available at the address specified in the contact information of the Controller. The above-mentioned letter will be stored and will be receivable by the Data Subject at the office of the Controller for a maximum of two months from the date of submission of the request.

9. What measures does the Controller use to ensure the protection of personal data?

9.1. The Controller ensures, reviews on a regular basis and improves the personal data protection measures in order to protect the personal data of individuals from unauthorised access, accidental loss, disclosure or destruction. To ensure this, the Controller shall use appropriate technical and organisational systems (for example, each employee is granted an individual right of access to information, the scope of the right of access is determined individually).

9.2. The Controller shall carefully check all service providers who process personal data of natural persons in the name and on behalf of the Controller. The Controller shall assess whether the cooperation partners (processors of personal data) ensure appropriate security measures so that the processing of personal data of natural persons takes place in accordance with the delegation of the Controller and the requirements of regulatory enactments.

9.3. In the event of a personal data security incident, if it may pose a high risk to the Data Subject's rights and freedoms, the Controller shall notify the Data Subject of such by using the contact information available to him/her (if possible), or the information will be published on the Controller's website www.virsi.lv or on social networks administered by the Controller, or otherwise (for example, through the media).

10. Final Provisions

10.1. This Statement shall be reviewed and updated periodically. The current version of the Statement shall enter into force on the date specified therein. The current version of the Statement is available on the website www.virsi.lv, as well as will be available at the places of performance of commercial activity of the Controller.

10.2. This Privacy Statement shall enter into force on 9 November 2021.