APPROVED BY

Chief Executive Officer

of UFS Ltd.

_____ ____/E.A. Sapach/

_____ _____, 2022

PERSONAL DATA PROCESSING POLICY of UNIVERSAL FINANCIAL SYSTEM Limited Liability Company

(the "Policy")

Moscow

2022

1. GENERAL PROVISIONS

The Personal Data Processing Policy of UFS Ltd. (the "Policy") is developed in accordance with Federal Law No. 152-FZ dated July 27, 2006 "On Personal Data" (the "Federal Law No. 152") and Regulation (EU) No. 2016/679 of the European Parliament and the Council of the European Union "On the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and on the Repeal of Directive 95/46/EU" (General Data Protection Regulation), and other regulations of the Russian Federation.

This Policy defines the procedure for processing personal data and measures ensuring the security of personal data by UFS Ltd. (the "Company") to protect the rights and freedoms of man and citizen when processing his/her personal data, including the rights to personal and family privacy.

Contact details:

Data operator name	UNIVERSAL FINANCIAL SYSTEM Limited Liability Company
Registered office	Moscow, Novy Arbat str., 21
Contacts	telephone: 8 (495) 269-83-66 e-mail: it@ufs.travel, support@ufs.travel

The following basic definitions are used in the Policy:

automated personal data processing - means personal data processing using computer facilities;

personal data blocking - means temporary suspension of personal data processing (unless such processing is necessary to clarify personal data);

personal data system - means a set of personal data, contained in databases, and information technologies and technical means ensuring their processing;

personal data depersonalization - means actions that make it impossible, without the use of additional information, to determine the belonging of personal data to a particular personal data subject;

personal data processing - means any action (operation) or set of actions (operations) performed with the use of automation tools or without the use of such means, including collection, recording, systematization, accumulation, storage, clarification (updating, modification), retrieval, use, transfer (distribution, provision of access), depersonalization, blocking, deletion, and destruction of personal data;

data operator - means a state authority, municipal authority, legal entity or individual that independently or together with other entities organizes and/or performs the personal data processing and determines the purposes of personal data processing, the composition of personal data to be processed, and actions (operations) to be performed with personal data;

personal data - mean any information relating to a directly or indirectly identified or identifiable individual (personal data subject);

provision of personal data - means actions aimed at disclosure of personal data to a certain person or a certain circle of persons;

personal data dissemination - means actions aimed at disclosure of personal data to an indefinite circle of persons (transfer of personal data) or familiarization with personal data of an

unlimited circle of persons, including publication of personal data in mass media, placement in information and telecommunication networks, or providing access to personal data in any other way;

cross-border transfer of personal data - means transfer of personal data to an authority, individual or legal entity located in a foreign country;

personal data destruction - means actions that make it impossible to restore the content of personal data in the personal data system and/or that destroy tangible media of personal data;

data controller - means an individual, legal entity, state authority, agency or other body that, independently or jointly with others, determines the purposes and means of processing personal data;

data processor - means an individual, legal entity, state authority, agency or other body that processes personal data on behalf of the data controller.

Services of the Company - mean services of UFS Ltd. for purchase and reservation of electronic air tickets, aeroexpress train tickets, railway tickets, bus tickets, hotels, conclusion of insurance contracts, and other services provided by third parties (Service Providers) and offered by the Company to the Customers through the Company's Web System in real time.

Company's Web System - means a complex of software and hardware, the exclusive rights to which belong to the Company, intended for the purchase and return of electronic air tickets, railway tickets, aeroexpress train tickets, bus tickets, insurance policies, hotel reservations, and other services provided by third parties (Service Providers) and offered by the Company to the Customers through the Company's Web System in real time on the Company's Website and in the Company's Mobile Application.

Company's Website - means an Internet site located at https://www.ufs-online.ru/.

Mobile Application - means the iSapsan mobile application or the Railway Tickets mobile application.

The Company shall publish or otherwise provide unrestricted access to this Personal Data Processing Policy in accordance with Part 2 of Article 18.1 of Federal Law No. 152.

2. PURPOSES OF COLLECTING PERSONAL DATA

2.1. Keeping records of the Company's employees in accordance with the requirements of laws and other regulations, assisting them in their career development, employment, training, health insurance, and providing them with other benefits and compensations.

2.2. Executing transactions for the sale of the Company's Services to the personal data subjects as well as other transactions made between UFS Ltd. and the personal data subjects.

2.3. Informing the personal data subjects about tariffs and discounts of carriers, sending advertising and information materials by mail, and conducting statistical research.

2.4. Performing contracts concluded between the Counterparties and the Company.

3. LEGAL GROUNDS FOR PERSONAL DATA PROCESSING

- Federal laws and regulations adopted on their basis that regulate relations associated with the Company's activities;
- Requirements of the Carriers/Service Providers in the field of railway and air transportation, insurance, etc.;
- Public Offer Agreement on Service Delivery Using the UFS Ltd. Online Service;

- Consent to Personal Data Processing posted on the Company's Websites (https://www.ufs-online.ru/ and https://www.ufs-partner.ru/) and in the Mobile Application;
- Consent to receive promotional discount codes and other advertising and information materials posted on the Company's Website (https://www.ufs-online.ru/) and in the Mobile Application;
- Contracts concluded between the Counterparties and the Company.

4. CATEGORIES OF PERSONAL DATA SUBJECTS

4.1. The Company processes personal data of the following categories of personal data subjects:

- Company's Customers – individuals who have been or are in contractual and other civil relations with the Company;
- Counterparties' customers – individuals who have entered into a contract with the Company's Counterparties and whose personal data are transferred by the Counterparties to the Company under contracts concluded between the Company and the Counterparties;
- Counterparties – individuals providing services to the Company on a contractual basis;
- candidates for vacant positions ("candidates") – individuals applying for vacant positions in the Company;
- employees – individuals who are or have been in an employment relationship with the Company;

4.2. family members (close relatives) of employees ("family members") — individuals who are in family relations with employees of the Company. List of personal data of Customers/ Counterparties' customers

- last name, first name and patronymic;
- date of birth;
- ID document details;
- copy of the ID document (if necessary);
- gender;
- citizenship;
- contact phone number;
- e-mail address.

4.3. List of personal data of Counterparties

- last name, first name and patronymic;
- ID document details;
- phone number;
- e-mail address;
- taxpayer identification number (INN);
- bank details.

4.4. List of personal data of candidates

- last name, first name and patronymic;
- date of birth;
- place of birth;
- ID document details;
- registered address;
- marital status;
- education;
- employment history;

- previous places of work;
- military registration details;
- gender;
- contact phone number;
- e-mail address;
- social benefits.

4.5. List of personal data of employees

- last name, first name and patronymic;
- date of birth;
- place of birth;
- ID document details;
- registered address;
- marital status;
- education;
- employment history;
- previous places of work;
- military registration details;
- driver's license;
- individual insurance account number (SNILS);
- INN;
- gender;
- contact phone number;
- e-mail address;
- salary;
- social benefits;
- position;
- bank details.

4.6. List of personal data of employees' family members

- details of the document confirming the kinship;
- ID document details;
- last name, first name and patronymic;
- date of birth;
- gender.

5. PROCEDURE AND CONDITIONS OF PERSONAL DATA PROCESSING

5.1. Personal data processing principles

The processing of personal data by the Company is based on the following principles:

- legality, fairness and transparency of personal data processing for the personal data subject;
- limiting the processing of personal data to the achievement of specific, predetermined and legitimate purposes (purpose limitation principle);
- avoiding personal data processing that is incompatible with the purposes of personal data collection;
- avoiding any consolidation of databases containing personal data that are processed for purposes incompatible with each other;
- processing only those personal data, which meet the purposes of their processing;

- compliance of the content and scope of personal data processed with the declared purposes of processing;
- avoiding the processing of personal data excessive in relation to the declared purposes of their processing (data minimization principle);
- ensuring the accuracy, sufficiency and relevance of personal data in relation to the purposes of personal data processing (accuracy principle);
- destruction or depersonalization of personal data when the purposes of their processing have been achieved, or when it is no longer necessary to achieve these purposes, or if the Company can not eliminate the violations of personal data, unless otherwise provided for by federal law (principle of data storage limitation);
- ensuring the security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, taking appropriate technical or organizational measures (integrity and confidentiality principle).

5.2. Legality of personal data processing

The legality of personal data processing is based on compliance with the following requirements and conditions:

- the personal data subject has consented to the processing of his/her personal data for one or more purposes;
- processing is required to perform a contract;
- processing is required to perform the relevant obligations of the data controller;
- processing is required to protect the vital interests of the personal data subject.

5.3. Conditions of personal data processing

The Company processes personal data under at least one of the following conditions:

- Personal data are processed with the consent of the personal data subject to the processing of his/her personal data;
- Personal data processing is required to achieve purposes provided for by any international treaties of the Russian Federation or any laws, or to perform any functions, powers and obligations imposed on the data operator by the laws of the Russian Federation;
- Personal data processing is required for the administration of justice or the execution of an order of court or another body or official to be executed in accordance with the laws of the Russian Federation on enforcement proceedings;
- Personal data processing is required to perform a contract, under which the personal data subject is a party, beneficiary or guarantor, as well as to conclude a contract on the initiative of the personal data subject or a contract, under which the personal data subject will be a beneficiary or guarantor;
- Personal data processing is required to protect the life, health or vital interests of the personal data subject, if obtaining the consent of the personal data subject is impossible;
- Personal data processing is required to exercise rights and legitimate interests of the data operator or third parties or to achieve socially significant goals, provided that this does not violate rights and freedoms of the personal data subject;
- Personal data are processed, public access to which is provided by the personal data subject or at his/her request ("publicly available personal data");
- Personal data are processed, which are subject to publication or mandatory disclosure under the federal law.

5.4. List of operations with personal data

The Company performs the following operations with personal data:

- collection;
- recording;
- accumulation;
- systematization;
- storage;
- clarification;
- transfer;
- depersonalization;
- destruction.

5.5. Confidentiality of personal data

The Company and other persons who have received access to personal data shall not disclose personal data to third parties and not disseminate personal data without the consent of the personal data subject, unless otherwise stipulated by the federal law.

5.6. Publicly accessible sources of personal data

For information purposes, the Company may create publicly accessible sources of personal data, including reference books and address books. Publicly accessible sources of personal data may, with the written consent of the personal data subject, include the personal data subject's full name, date and place of birth, position, contact phone numbers, e-mail address, and other personal data.

Such personal data shall be removed from publicly accessible sources of personal data at any time at the request of the personal data subject or by decision of court or other authorized state bodies.

5.7. Special categories of personal data

The Company does not process special categories of personal data.

5.8. Biometric personal data

The Company does not process biometric personal data.

5.9. Assigning the personal data processing to third parties

The Company may assign the personal data processing to third parties (subprocessors) with the consent of the personal data subject, unless otherwise provided for by the federal law, on the basis of a contract concluded with this third party. The subprocessor that processes personal data on behalf of the Company shall comply with the principles and rules for personal data processing, as provided for in Federal Law No. 152.

The assignment shall contain:

- list of personal data;
- list of operations with personal data;
- purposes of personal data processing;
- subprocessor's obligations to ensure the confidentiality and security of personal data;
- subprocessor's obligations to comply with the requirements for localization of personal data (Part 5 of Article 18 of Federal Law No. 152);
- subprocessor's obligations to take measures provided for in Article 18.1 of Federal Law No. 152;

- subprocessor's obligations, at the request of the data operator, to provide documents and other information confirming the adoption of measures and compliance with the requirements prescribed by the law and the assignment;
- requirements for personal data protection in accordance with Article 19 of Federal Law No. 152, including the requirements to notify the data operator of unlawful and/or accidental transfer ("leakage") of personal data.

5.10. Transfer of personal data

Customer's personal data may be transferred to third parties only with the consent of the Customer (acceptance of the offer agreement), unless otherwise provided for by the laws of the Russian Federation.

The Company shall transfer Customers' personal data only to third parties that are in a contractual relationship with the Company and process the personal data on behalf of the Company, as well as to the authorized state bodies in accordance with the law.

Customers' personal data may be transferred to third parties as part of the provision of services for the sale of air and railway tickets and hotel reservations.

Third parties shall take all necessary organizational and technical measures to protect Customers' personal data against illegal or accidental access, destruction, modification, blocking, copying, provision, distribution and other illegal actions in accordance with the regulations on personal data protection. Third parties shall be responsible to the personal data subjects for following the procedures for storing, processing and ensuring confidentiality of personal data.

The Customers' personal data shall be transferred between units of the Company only by employees authorized to process personal data.

Information relating to the Customers' personal data may be provided to state bodies in accordance with the procedure established by federal laws.

If a person requesting the Customer's personal data is not authorized by federal law to collect such personal data, or if there is no written consent of the Customer to provide his/her personal data, the Company shall refuse to provide personal data. The requesting person shall be given a written refusal to provide personal data.

5.11. Cross-border transfer and processing of personal data

The Company shall make sure that the foreign country, to whose territory personal data are to be transferred, provides adequate protection of the rights of personal data subjects before such a transfer takes place.

Cross-border transfer of personal data to the territory of foreign states that do not provide adequate protection of the rights of personal data subjects may be performed in the following cases:

- the personal data subject has consented to cross-border transfer of his/her personal data;
- in cases provided for by international treaties of the Russian Federation;
- in cases provided for by federal laws, if it is necessary to protect the foundations of the constitutional order of the Russian Federation, to ensure the national defense and state security, to ensure the stable and safe functioning of the transport complex, and to protect the interests of individuals, society and the state in the field of the transport complex from acts of unlawful interference;
- performance of a contract to which the personal data subject is a party;

- protection of the life, health, or vital interests of the personal data subject or other persons if it is impossible to obtain the written consent of the personal data subject.

To perform the cross-border transfer of personal data, the Company shall:

1. Obtain the following information from the third party to whom the data are to be transferred:

- about the measures taken to protect the transferred personal data and about the conditions for termination of their processing;
- about the legal regulation of personal data issues, if personal data are transferred to countries that do not provide adequate protection for the personal data subjects;
- about the third party (name, telephone, postal address, e-mail address);

2. Assess the third party's compliance with the requirements for ensuring the confidentiality and security of personal data;

3. Submit to the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) a notice containing:

- name and address of data operator;
- date and number of the notice on personal data processing;
- full name of the person responsible for personal data processing (data protection officer), his/her contact details (phone number, postal address, e-mail address);
- legal basis and purpose of the cross-border transfer and further processing of personal data;
- categories and list of transferred personal data;
- categories of personal data subjects;
- list of foreign countries to which the data are to be transferred;
- date of assessment described in Clause 2 above.

4. When transferring to countries that provide adequate protection of personal data subjects — initiate the transfer after sending the notice;

5. When transferring to countries that do not provide adequate protection of personal data subjects — initiate the transfer after 10 business days, if Roskomnadzor has not made a decision to prohibit or restrict the transfer;

6. Ensure the destruction by third parties of personal data previously transferred to them if Roskomnadzor decides to prohibit or restrict the cross-border transfer of personal data.

5.12. Time limits for personal data processing

The Company shall store personal data of Customers only for the period necessary to achieve the relevant purposes, unless a longer period of storage of personal data is established by law.

Personal data processed by the Company shall be destroyed or depersonalized if:

- the purposes of personal data processing are achieved or there is no longer need to achieve those purposes;
- the personal data subject withdraws his/her consent to the processing of his/her personal data;
- the activities of UFS Ltd. are terminated.

For personal data subjects who are EU citizens, the personal data storage period shall be 30 days.

5.13. Storage of personal data

All databases of UFS Ltd. are geographically distributed and located in the Russian Federation.

5.14. Update, correction, deletion and destruction of personal data

If it is confirmed that the personal data are inaccurate or improperly processed by the Company, the personal data shall be updated and the processing shall be stopped.

If the purposes of personal data processing are achieved, or if the personal data subject withdraws his/her consent to their processing, the personal data shall be destroyed:

- unless otherwise provided for by a contract, under which the personal data subject is a party, beneficiary or guarantor;
- if the data operator is not entitled to perform processing without the consent of the personal data subject on the grounds provided for by the Federal Law "On Personal Data" or other federal laws;
- unless otherwise provided for by another agreement between the data operator and the personal data subject.

5.15. Procedure for responding to requests from personal data subjects, their representatives and authorized bodies

When the personal data subject or his/her legal representative requests in writing or electronically for access to his/her personal data, the Company shall be guided by the requirements of Articles 14, 18 and 20 of Federal Law No. 152-FZ, and Regulation (EU) No. 2016/679 of the European Parliament and the Council of the European Union "On the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and on the Repeal of Directive 95/46/EU" (General Data Protection Regulation).

Depending on the information provided in the request, a decision shall be made on granting the personal data subject an access to his/her personal data.

If the information provided by the personal data subject is insufficient to determine his/her identity or the provision of personal data violates the constitutional rights and freedoms of others, the Company shall prepare a reasoned response containing a reference to Part 8 of Article 14 of Federal Law No. 152-FZ or other federal law that constitutes the basis for such refusal within ten business days from the date of the request of the personal data subject or his/her legal representative.

Information on the availability of personal data is provided to the subject when responding to the request within ten business days after receipt of the request of the personal data subject or his legal representative.

Responses to personal data subjects' requests regarding the processing of their personal data in accordance with Part 7 of Art. 14 of Federal Law No. 152 shall be sent through the same channel (e-mail, personal account on the website, etc.), through which the request was received, unless otherwise specified in the request. In response to these requests, "the information about the ways to fulfill the obligations established by Article 18.1 of Federal Law No. 152" shall be also sent. Upon receipt of personal data not from the personal data subject, the list of received personal data shall be additionally sent to the personal data subject.

In accordance with Part 4 of Article 20 of Federal Law No. 152-FZ, the Company may submit to the authorized body for protection of rights of personal data subjects, upon request, the information required for its activities within ten business days after receipt of such request. A request of such authority may be sent in an electronic form.

6. RIGHTS OF THE PERSONAL DATA SUBJECTS

6.1. Consent of the personal data subject to the processing of his/her personal data

The personal data subject decides to provide his/her personal data and consent to their processing freely, willingly and in his/her own interest. The consent to personal data processing may be given by the personal data subject or his/her representative in any form that allows confirming the fact of its receipt unless otherwise prescribed by federal law.

The Customer provides the Company with his/her personal data for the provision of the Services by the Company.

By ticking the field "I give my consent to the processing of personal data" on the Company's Website and/or in the Mobile Application, when ordering the Company's Services, the Customer gives his/her consent to the processing of personal data.

The text of the Consent to Personal Data Processing is available publicly in electronic form on the Company's Website and in the Company's Mobile Application. Without consent to the processing of personal data, the receipt of the Company's Services and the use of the Company's Mobile Application and/or Website is impossible.

When the Customer orders the Services on the Partner's website or at air/railway ticket sales desks, the Partner shall be responsible for obtaining the Customer's consent to the processing of personal data. In this case, the Partner shall entrust the processing of Customers' personal data to UFS Ltd. under existing contracts and transfer them in electronic form. There is no need for the Company to additionally obtain consent to the processing of personal data.

The Counterparty's personal data shall be provided by the Counterparty in the performance of a relevant contract.

According to Clause 5 of Part 1 of Article 6 of Federal Law No. 152, personal data of Counterparties may be processed by the Company without their written consent, if the processing of personal data is necessary for the performance of a contract to which the Counterparty is a party.

The obligation to provide evidence of the personal data subject's consent to the processing of his/her personal data or evidence of existence of the grounds specified in Federal Law No. 152 is imposed on the Company.

6.2. Rights of the personal data subject

The Company shall offer the Customer various options for controlling the use of his/her personal data. The Customer may change, clarify, upload in any available format and delete his/her personal data by refusing from the data processing.

The personal data subject may receive from the Company information about the processing of his/her personal data, if such a right is not limited in accordance with federal laws. The personal data subject may demand that the Company clarify, change, block or destroy his/her personal data if they are incomplete, outdated, inaccurate, illegally obtained or are not required for the declared purpose of processing, as well as take any measures provided for by the laws to protect his/her rights.

The personal data subject may change or delete any of his/her personal data at any time, as well as upload them in any proposed format.

The processing of personal data for the purposes of promoting goods, works, services on the market by direct contact with a potential consumer by means of communication, as well as for the purposes of political agitation, is allowed only with the prior consent of the personal data subject. The said processing of personal data is recognized to be performed without the prior consent of the personal data subject, unless the Company proves that such consent has been obtained.

The Company shall immediately stop the processing of personal data for the aforementioned purposes at the request of the personal data subject.

It is prohibited to make decisions based on solely automated personal data processing that create legal consequences with respect to the personal data subject or otherwise affect his/her rights and legitimate interests, unless otherwise provided by federal laws, or the consent in writing of the subject of personal data is obtained.

If the personal data subject believes that the Company processes his/her personal data in violation of Federal Law No. 152 and other legislative acts or otherwise violates his/her rights and freedoms, the personal data subject may appeal against the actions or omissions of the Company to the authorized body for protection of rights of personal data subjects or to court.

The personal data subject may protect his/her rights and legitimate interests, including compensation for damage and/or moral damage in court.

7. SECURITY OF PERSONAL DATA

The security of personal data processed by the Company shall be ensured by taking legal, organizational and technical measures prescribed by the federal laws on personal data protection.

To prevent unauthorized access to personal data, the Company shall take the following organizational and technical measures:

- appointing officials responsible for the processing and protection of personal data;
- issuing the data operator's personal data processing policy, local regulations on issues of personal data processing, as well as local regulations on procedures for preventing and detecting violations of the laws of the Russian Federation and eliminating the consequences of such violations;
- limiting the number of persons having access to personal data;
- establishing rules for access to personal data processed in personal data systems, as well as ensuring the registration and recording of all operations performed with personal data in personal data systems;
- familiarizing the personal data subjects with the requirements of the federal laws and regulations of the Company on the processing and protection of personal data;
- familiarizing the Company's employees, who directly process personal data, with the personal data laws of the Russian Federation, including the personal data protection requirements, the Company's personal data processing policy, and the local regulations on issues of personal data processing;
- organizing registration, storage and circulation of data carriers;
- defining the threats to personal data security, and creating a threat model on their basis;
- developing a personal data protection system based on the threat model;
- checking the readiness and effectiveness of the information protection tools;
- control of user access to information resources and software and hardware used for personal data processing;
- registering and recording the actions of users of personal data systems;
- use of the information protection tools that have passed the conformity assessment procedure;
- use of anti-virus and recovery tools of the personal data protection system;
- use of firewall, intrusion detection, security analysis, and cryptographic data security tools, when necessary;
- data encryption, when necessary;
- personal data traffic encryption (HTTPS, IPSec, TLS, PPTP, SSH)

- use of information security event monitoring tools;
- use of two-factor authentication to administer data security tools;
- detecting unauthorized access to personal data, and taking measures to detect, prevent and eliminate the consequences of computer attacks on personal data systems and to respond to computer incidents in them;
- restoring personal data modified or destroyed due to an unauthorised access to them;
- control over the measures taken to ensure personal data security and over the security level of personal data systems;
- internal control and/or audit of compliance of personal data processing with the laws of the Russian Federation and regulations adopted based on them, requirements for the personal data protection, and the data operator's personal data processing policy and local regulations;
- control of access to the Company's facilities, supervision of premises where technical means of personal data processing are located;

assessment of the harm that may be caused to personal data subjects in the event of a violation of the law, as well as the ratio of the said harm to the measures taken by the data operator to ensure the fulfillment of obligations.

8. NOTIFICATION OF ROSKOMNADZOR OF ILLEGAL OR ACCIDENTAL TRANSFER (PROVISION, DISSEMINATION, ACCESS) (LEAKAGE) OF PERSONAL DATA

The Company shall notify Roskomnadzor of the facts of "illegal or accidental transfer (provision, distribution, access) of personal data, which resulted in violation of the rights of the personal data subjects." In this case, the information shall be sent within two periods:

- Within the first 24 hours after the detection of such an incident — information about the incident itself, the alleged harm to personal data subjects, the measures taken to eliminate it, and the contact details of the person authorized to interact with Roskomnadzor.
- Within 72 hours after the detection of an incident — additional information about the internal investigation conducted and the persons whose actions caused the incident (if any).

The "illegal or accidental transfer of personal data" includes any situation when personal data were provided to a third party or distributed on the Internet or when access to personal data was obtained by a third party, if there were no legal grounds for the listed actions.

9. FINAL PROVISIONS

Other rights and obligations of the Company as the data operator are determined by the personal data laws of the Russian Federation, and Regulation (EU) No. 2016/679 of the European Parliament and the Council of the European Union "On the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and on the Repeal of Directive 95/46/EU".

Company's officers guilty of violating the rules for the processing and protection of personal data shall bear financial, disciplinary, administrative, civil or criminal liability in accordance with the procedure established by federal laws.

Appendix 1. Form of Request for Clarification of Personal Data

To the data operator:

UFS Ltd.

Registered office:

119019, Moscow, Novy Arbat str., 21

from_____

(full name)

passport series _____ number_____ issued on by _____

(date of issue)

_____

(name of the issuing authority)

REQUEST

for Clarification of Personal Data

In accordance with _____, I request that my personal data be modified based on the information contained in the following documents:

_____.

and, if necessary, blocked for the time that these modifications are made.

Please inform me of the results of the clarification at the following address:

_____.

_____ _____

(date) (signature)

Appendix 2. Form of Request for Withdrawal of Consent to Personal Data Processing

To the data operator:

UFS Ltd.

Registered office:

119019, Moscow, Novy Arbat str., 21

from_____

(full name)

Passport series_____ number_____ issued on by_____

(date of issue)

_____

(name of the issuing authority)

WITHDRAWAL

of Consent to Personal Data Processing

In accordance with _____, I request that you stop processing my personal data, namely:

_____,

(list of operations with personal data for which the consent is withdrawn)

_____,

(list of personal data)

performed for the purposes of

_____,

(purposes of personal data processing)

due to

_____.

(reason for withdrawal)

Please inform me of the results at the following address:

_____.

_____ _____

(date) (signature)

Appendix 3. Form of Request for Personal Data Processing Information

To the data operator:

UFS Ltd.

Registered office:

119019, Moscow, Novy Arbat str., 21

from _____

(full name)

passport series_____ number _____issued on by_____

(date of issue)

_____

(name of the issuing authority)

REQUEST

for Information about the Personal Data Processing

In connection with the processing by UFS Ltd. of personal data obtained

_____

(number and date of the contract; other information confirming the fact of personal data processing by the data operator)

in accordance with _____, I request that you send me the following information:

1) confirmation of the fact of personal data processing by the data operator;
2) legal grounds and purposes of personal data processing;
3) purposes and methods of personal data processing used by the data operator;
4) name and location of the data operator, information on persons (except for employees of the data operator) who have access to personal data or to whom personal data may be disclosed on the basis of a contract with the data operator or by virtue of federal law;
5) list of the processed personal data and their source;
6) time limits of personal data processing, including time limits of their storage;
7) procedure for exercising my rights provided for by the Federal Law "On Personal Data";
8) information on the performed or expected cross-border transfer of personal data;
9) full name and address of the person who processes personal data on behalf of the data operator, if the processing is or will be entrusted to such person;

at the following address:

_____

_____ _____

(date) (signature)