POLICY
for processing and ensuring the security of personal data at PJSC RussNeft

Moscow
2023

1. General

The policy for processing and ensuring the security of personal data (hereinafter referred to as PD) at PJSC RussNeft (hereinafter referred to as the Policy) is a local regulatory act of PJSC RussNeft (hereinafter referred to as the Company), developed in accordance with Clause 2, Part 1 of Art. 18.1 of the Federal Law No. 152-FZ dated July 27, 2006 "On Personal Data" and defines the basic principles, goals and conditions for processing PD, as well as measures to protect PD in the Company.

Control over compliance with the requirements of this Policy is carried out by the Person Responsible for organizing the processing of PD.

This Policy has been developed in order to implement the requirements of the legislation of the Russian Federation in the field of Processing and ensuring security of PD and is aimed at ensuring the protection of the rights and freedoms of an individual and citizen when processing his/her PD, including the protection of rights to privacy, personal and family secrets.

The Company has the right to make changes to the Policy in compliance with the requirements of the legislation of the Russian Federation and regulatory legal acts.

2. Terms and definitions

Automated processing of PD is processing of PD using computer technology.

PD security is a state of PD protection in which their confidentiality, availability and integrity are ensured.

PD blocking is a temporary cessation of PD Processing (except for cases where processing is necessary to clarify PD).

Personal Data Information System (PDIS) is a set of information technologies and technical means contained in PD databases and ensuring their processing.

Confidentiality of PD is a mandatory requirement for a person who has gained access to PD not to transfer such PD to third parties without the consent of its owner.

Unauthorized access (UNA) is access to PD or actions with PD that violate the rules of access control using the means provided by the PDIS.

PD carrier is technical devices intended for recording and processing PD as part of computer equipment, as well as for storing and moving recorded PD outside the computer equipment, as well as paper PD media.

PD Processing is any action (operation) or set of actions (operations) performed using

automation tools or without the use of such tools with PD, including collection, recording, systematization, accumulation, storage, clarification (updating, changing), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of PD.

PD Processing without the use of automation means is actions with PD, such as use, clarification, distribution, destruction of PD in relation to each of the PD Subjects, carried out with the direct participation of a person.

Person responsible for ensuring the PD security is the person responsible for ensuring PD security, for the implementation and continuity of compliance with established protection measures and monitoring the functioning of information security tools used in the Company's PDIS.

Person responsible for organizing the PD Processing is the person exercising internal control over compliance by the Company and its employees with the legislation of the Russian Federation on PD, including requirements for the protection of PD.

Personal data (PD) are any information relating to a directly or indirectly identified or identifiable individual (PD Subject).

PD authorized by the subject of PD for distribution are PD, access to an unlimited number of persons to which is provided by the PD Subject by giving consent to the processing of PD authorized by the PD Subject for distribution in the manner prescribed by the Federal Law “On Personal Data”.

Providing PD is actions aimed at disclosing PD to a certain person or a certain circle of persons.

Company employee is a person who carries out his/her activities in the Company on the basis of an employment contract and has potential access to the processing of PD, both with and without the use of automated PD processing tools.

PD protection system (PDPS) is a set of organizational and technical measures determined based on the current threats to the security of PD and information technologies used in PDIS.

Information security tools (IST) are technical, software, and hardware tools designed or used to protect information.

PD Subject is an individual who is directly or indirectly identified or identifiable using PD.

Authorized body for the protection of the rights of PD Subjects is a federal executive body that exercises the functions of control and supervision over the compliance of PD Processing with the requirements of the legislation of the Russian Federation in the field of PD.

Federal Law "On Personal Data" is Federal Law of July 27, 2006 No. 152-FZ "On Personal Data".

Other terms, the meaning of which is not defined in this Policy, are used in the meaning given to them by the legislation of the Russian Federation and regulations.

3. PD Processing principals

Processing of PD by the Company is carried out on the basis of the following principles:

- legality and fairness (compliance with legislative acts and compliance with the equal interests of PD Subjects, without abusing the opportunities presented on the basis of information provided by the PD Subject) of the purposes and methods of PD Processing;
- compliance of the purposes of PD Processing with legitimate purposes, pre-determined and declared when collecting PD;
- compliance of the volume and content of the processed PD with the methods and purposes of PD Processing;
- accuracy of PD, their sufficiency and relevance in relation to the purposes of PD Processing;
- inadmissibility of processing PD that is excessive in relation to the purposes stated when collecting PD;
- inadmissibility of combining databases containing PD, the processing of which is carried out for purposes incompatible with each other;
- storage of PD in a form that makes it possible to identify the PD Subject, no longer than required by the purposes of PD Processing, or the PD storage period established by the legislation of the Russian Federation, an agreement concluded by the Company with the PD Subject, consent to PD Processing (hereinafter referred to as the PD storage period);
- destruction of PD upon achievement of the purposes of their processing, if the storage period for PD is not established by the legislation of the Russian Federation, an agreement to which the PD Subject is a party, beneficiary or guarantor.

4. Purposes and legal grounds for PD Processing

The company collects and processes PD for the following purposes:

- protection of life, health or other important interests of PD Subjects;
- conclusion, execution and termination of civil contracts with individuals, legal entities, individual entrepreneurs and other persons, in cases provided for by law and the Company's Articles of Association;
- organizing personnel records, ensuring compliance with laws and other regulations, concluding and fulfilling obligations under labor and civil contracts;

- conducting personnel records management, assisting employees in employment, training and personnel transfer within the framework of the staffing table, using various types of benefits, fulfilling the requirements of tax legislation in connection with the calculation and payment of personal income tax, as well as the unified social tax, pension legislation in the formation and submission of personalized data about each recipient of income taken into account when calculating insurance premiums for compulsory pension insurance and security, filling out primary statistical documentation in accordance with the Labor and Tax Codes of the Russian Federation, federal laws;
- organizing and conducting internships for students in higher vocational training and secondary vocational training programs;
- implementation of the access control regime in the Company, ensuring the safety of property;
- disclosure of information about management bodies, maintaining the necessary corporate and shareholder documentation in accordance with the legislation of the Russian Federation;
- generation of reference materials for internal information support of the activities of the Company, its branches, companies included in the corporate structure of the Company, interdependent legal entities;
- execution of judicial acts, acts of other bodies or officials subject to execution in accordance with the legislation of the Russian Federation;
- issuing powers of attorney to representatives of organizations involved in the implementation of Company's projects;
- performing other actions that do not conflict with the legislation of the Russian Federation.

The grounds for processing the PD of the Company's PD Subjects include the following:

- Civil Code of the Russian Federation;
- Tax Code of the Russian Federation;
- Labor Code of the Russian Federation;
- Federal Law No. 149-FZ dated July 27, 2006 "On information, information technologies and information security";
- Federal Law No. 152-FZ dated July 27, 2006 "On Personal Data";
- Federal Law No. 27-FZ dated April 1, 1996 "On individual (personalized) registration in the compulsory pension insurance system";
- Federal Law No. 223-FZ dated July 18, 2011 "On the procurement of goods, works, services by certain types of legal entities";
- Federal Law No. 255-FZ dated December 29, 2006 "On compulsory social insurance in case of temporary disability and in connection with maternity";
- Federal Law No. 402-FZ dated December 6, 2011 "On Accounting";

- Federal Law No. 115-FZ dated August 7, 2001 “On combating the legalization (laundering) of proceeds from crime and the financing of terrorism”;
- Decree No. 687 of the Government of the Russian Federation dated September 15, 2008 “On approval of the Regulations on the specifics of PD Processing carried out without the use of automation tools”;
- Decree No. 1119 of the Government of the Russian Federation dated November 1, 2012 “On approval of requirements for the protection of personal data during their processing in personal data information systems” (hereinafter referred to as Decree No. 1119 of the Government of the Russian Federation);
- Articles of Association of the Company.

The Company carries out Automated processing of PD and Processing of PD without the use of automation tools by collecting, recording, systematizing, accumulating, storing, clarifying (updating, changing), extracting, using, transferring (providing, providing, accessing), blocking, deleting, destroying PD.

The Company in its activities proceeds from the fact that when interacting with the Company, the PD Subject provides accurate and reliable information about his/her PD, and also promptly notifies the Company of changes in his/her PD.

5. Categories of PD and PD Subjects

The company processes PD of the following categories of PD Subjects:

- employees;
- candidates for employment;
- counterparties (individuals, employees of counterparties);
- trainees;
- employees of third-party organizations (within the framework of contractual relations);
- visitors of the Company;
- members of the Board of Directors.

In accordance with the provisions of Decree No. 1119 of the Government of the Russian Federation, the Company processes the following categories of PD without the use of automation tools and with the use of automation tools:

- other categories of PD – PD not classified into categories: special, biometric and public PD;
- biometric categories of PD – information that characterizes the physiological and biological characteristics of a person.

Complete list of PD and categories of PD Subjects is approved by the List of processed PD.

6. Terms for processing the personal data of PD Subjects and terms for transferring the PD to third parties

The Company processes PD of PD Subjects in accordance with the Company's local regulations, developed in accordance with the requirements of the legislation of the Russian Federation in the field of PD.

Processing of PD in the Company is permitted in the following cases:

- PD Processing is carried out with the consent of the PD Subject to the processing of his/her PD;
- PD Processing authorized by the PD Subject for distribution is carried out with consent to the processing of PD authorized by the PD Subject for distribution, submitted by the PD Subject separately from other consents of the PD Subject to the processing of his/her PD;
- PD Processing is necessary in connection with the participation of a person in constitutional, civil, administrative, criminal or arbitration proceedings; for the execution of a judicial act, an act of another body or official, subject to execution in accordance with the legislation of the Russian Federation;
- PD Processing is necessary for the execution of an agreement to which the PD Subject is a party or beneficiary or guarantor, as well as for concluding an agreement on the initiative of the PD Subject;
- PD Processing is carried out for statistical or other research purposes, except for the cases established in Art. 15 of Federal Law "On Personal Data", subject to mandatory depersonalization of PD;
- Processing of PD received from open sources posted by the PD Subject or at his request;
- Processing of PD subject to publication or mandatory disclosure in accordance with federal law.

Unless otherwise provided by federal law, the Company has the right to entrust the processing of PD to another person on the basis of an agreement concluded with this person, subject to the consent of the PD Subject. A person processing PD on behalf of the Company is obliged to comply with the principles and rules for processing PD provided for by the Federal Law "On Personal Data".

The instruction to a third party specifies the purposes of processing and a list of actions (operations) with PD that can be performed by this person, establishes his/her responsibilities to ensure the Confidentiality of PD and the Security of PD during their processing, as well as requirements for the protection of processed PD in accordance with the Federal Law "On personal data."

The Company does not carry out cross-border transfer of PD (transfer to the territory of countries that provide adequate protection of PD with the consent of the PD Subject).

The Company does not make decisions that give rise to legal consequences in relation to PD Subjects or otherwise affect their rights and legitimate interests, based solely on Automated PD Processing, except in the case of written consent of the PD Subject or in cases provided for by federal laws that also establish measures to ensure compliance with the rights and legitimate interests of the PD Subject.

The company stops processing PD in the following cases:

- upon detection of unlawful Processing of PD carried out by the Company or a person acting on behalf of the Company. The Company, within a period not exceeding three business days from the date of such detection, terminates the unlawful Processing of PD or ensures the termination of unlawful Processing of PD by a person acting on behalf of the Company and eliminates the violations committed. If it is impossible to eliminate the violations committed, the Company, within a period not exceeding ten business days from the date of detection of illegal actions with PD, destroys PD or ensures its destruction. The Company notifies the PD Subject or his representative about the elimination of violations or the destruction of PD, and if the appeal or request was sent to the authorized body for the protection of the rights of PD Subjects, also this body;
- upon achieving the goal of PD Processing, the Company stops PD Processing or ensures its termination (if PD Processing is carried out by another person acting on behalf of the Company) and destroys PD or ensures their destruction (if PD Processing is carried out by another person acting on behalf of the Company) on time, not exceeding thirty days from the date of achieving the goal of PD Processing, unless otherwise provided by an agreement to which the PD Subject is a party, beneficiary or guarantor, another agreement between the Company and the PD Subject, or if the Company does not have the right to carry out PD Processing without the consent of the PD Subject on the grounds provided for by the Federal Law “On Personal Data” or other federal laws.
- when the PD Subject withdraws consent to the processing of his/her PD, the Company stops PD Processing or ensures its termination (if PD Processing is carried out by another person acting on behalf of the Company) and if the preservation of PD is no longer required for the purposes of PD Processing, destroys the PD or ensures their destruction (if PD Processing is carried out by another person acting on behalf of the Company) within a period not exceeding thirty days from the date of receipt of the said response, unless otherwise provided by the agreement to which the PD Subject is a party, beneficiary or guarantor, or another agreement between the Company and the PD Subject or if the Company does not have the right to process PD without the consent of the PD Subject on the grounds provided for by the Federal Law “On Personal Data” or other federal laws.

If it is not possible to destroy PD within the period specified in this section, the Company blocks such PD or ensures their blocking (if the processing of PD is carried out by another

person acting on behalf of the Company) and ensures the destruction of PD within a period of no more than six months, if no other period is established by federal laws.

7. Consent to PD Processing

Receiving and Processing of PD in cases stipulated by the Federal Law "On Personal Data" is carried out by the Company with the consent of the Subject of PD. Consent to the PD Processing may be given by PD Subject or his representative in any form that allows confirming the fact of its receipt, unless otherwise established by federal law. If consent to the PD Processing was obtained from a representative of PD Subject, the powers of this representative to give consent on behalf of PD Subject are verified by the Company.

In cases provided for by the Federal Law "On Personal Data", PD processing shall be carried out by the Company only with the written consent of PD Subject. Consent in the form of an electronic document signed with an electronic signature in accordance with Federal Law No. 63-FZ of 06.04.2011 "On Electronic Signature" is considered equivalent to a written consent on paper containing PD Subject's handwritten signature.

The written consent of PD Subject shall include:

- surname, first name, patronymic, address of PD Subject, number of the main identification document, information about the date of issue of the specified document and the issuing authority;
- surname, first name, patronymic, address of the representative of PD Subject, number of the main identification document, information about the date of issue of the specified document and the issuing authority, details of a power of attorney or other document confirming the powers of this representative (upon receipt of consent from the representative of PD Subject);
- Company name and address;
- purpose of PD processing;
- the list of PD, for the processing of which the consent of PD Subject is given;
- name or surname, first name, patronymic and address of the person processing the PD on behalf of the Company, if the PD processing is entrusted to such a person;
- a list of actions with PD for which consent is given, a general description of the methods used by the Company for PD processing;
- the period during which the consent is valid, as well as the method of its withdrawal, unless otherwise established by federal law;
- signature of PD Subject.

PD Subject gives the Company consent to PD Processing freely, at his own will and in his own interest. Consent to the PD processing may be revoked by PD Subject by sending a written application to the Company in a free form. In this case, the Company undertakes to

stop processing, as well as destroy all PD available in the Company within the time limits stipulated in the Federal Law "On Personal Data".

The transfer of PD to third parties shall be carried out by the Company with the consent of PD Subject in accordance with the requirements of the legislation of the Russian Federation. Consent to the processing of PD, authorized by PD subject for distribution, is issued separately from other consents of PD Subject to the processing of his personal data. The requirements for the content of consent to the processing of PD authorized by PD Subject for distribution are established by the authorized body for the protection of PD Subjects rights.

8. The Rights of PD Subjects

In order to ensure the protection of PD Subjects rights established by law, the Company has developed and introduced a procedure for dealing with appeals and requests from PD Subjects, as well as the procedure for providing PD Subjects with information prescribed by the legislation of the Russian Federation on personal data.

PD Subject or his legal representative has the right to receive information concerning the PD Processing, including:

- confirmation of PD Processing by the Company;
- legal grounds for and purposes of PD Processing;
- goals and methods used by the Company for PD processing;
- name and location of the Company, information about persons (other than the Company employees) with access to PD or to whom PD may be disclosed on the basis of an agreement with the Company or on the basis of federal law;
- processed PD related to the relevant PD Subject, the source of their obtainment, unless another procedure for submitting such data is provided by federal law;
- timeline of PD processing, including the period of their storage;
- the procedure whereby PD Subject exercises the rights provided for by the Federal Law "On Personal Data";
- information about the implemented or prospective cross-border transfer of PD;
- the name or surname, first name, patronymic and address of the person in charge of PD processing on behalf of the Company, if processing is or will be entrusted to such a person;
- other information provided for by the Federal Law "On Personal Data" or other federal laws on PD.

The Company provides the specified information upon application or on the basis of a relevant written request of PD Subject or his representative, containing the following: the number of the main identity document of PD Subject or his representative; information about the date of issue of the specified document and the issuing authority; information

confirming the participation of PD Subject in relations with the Company (contract number, date of the contract, reference code and (or) other information), or information otherwise confirming the fact of PD Processing by the Company, signature of PD Subject or his representative.

A PD Subject shall have the right to require the Company to amend PD, block or destroy them if the PD is incomplete, outdated, inaccurate, illegally obtained or is not necessary for the stated purpose of PD Processing, as well as to take measures provided for by PD laws of the Russian Federation to protect his rights.

In order to exercise and protect their rights and legitimate interests in terms of ensuring the legality of PD Processing and ensuring the PD Security, the PD Subject has the right to contact the Company.

If PD Subject believes that the Company processes PD in violation of the requirements of the Federal Law "On Personal Data" or otherwise violates his rights and freedoms, PD Subject has the right to appeal the actions or inaction of the Company to the Authorized Body for the Protection of PD Subject Rights or in court.

The right of PD Subject to access to his PD may be restricted in accordance with federal laws, including if PD Subject's access to his PD violates the rights and legitimate interests of third parties.

9. Rights and obligations of the Company

The Company shall be entitled to:

- advocate its interests in the judiciary;
- provide PD of Subjects to the third parties, if this is stipulated by the legislation of the Russian Federation (law enforcement, tax authorities, etc.);
- refuse to provide PD in cases stipulated by the legislation of the Russian Federation;
- use the PD of PD Subject without his consent, in cases stipulated by the legislation of the Russian Federation.

Responsibilities of the Company:

- ensure Confidentiality with respect to personal data that have become known to the Company in the course of its activities;
- in the event of detecting illegal Processing of PD, inaccuracy of PD, block illegally processed PD related to this PD Subject, or ensure their blocking (if PD processing is carried out by another person acting on behalf of the Company) at the request of a PD Subject or his representative, or at the request of a PD Subject or his representative, from the moment of such request;
- terminate PD Processing or ensure its termination (if PD processing is carried out by another person acting on behalf of the Company) and destroys PD or ensures their destruction (if PD processing is carried out by another person acting on behalf of the

Company), if the purpose of PD processing is achieved.

10. Personal data security

To ensure the PD security, the Company takes the necessary and sufficient measures of organizational and technical nature to protect PD of PD Subjects from unauthorized or accidental access to them, destruction, modification, blocking, copying, distribution, as well as from other illegal actions, including, inter alia:

- appointment by order of the Company of the Person Responsible for the organization of PD processing and Person Responsible for PD Security, as well as determining of their functions and powers;
- development of and keeping up-to-date the Company's internal regulatory documents regarding the PD Processing, the PD Security, establishing of the procedures aimed at identifying and preventing violations of the legislation of the Russian Federation on PD by the Company, elimination of the consequences of such violations;
- periodic internal control, as well as control carried out by third parties (external audit) under a contract of work and labor and service contact, compliance of PD Processing with the requirements of the Federal Law "On Personal Data" and of regulatory legal acts adopted in accordance with it;
- conducting an assessment of the harm that may be caused to PD Subjects in the event of a violation of the legislation on PD, as well as of the adequacy of the measures taken to ensure the compliance with PD-legislation to the harm caused;
- familiarization of the Company's Employees directly engaged in the PD Processing with the provisions of the legislation of the Russian Federation and internal regulatory documents of the Company regarding the PD Processing and PD Security, training of these Employees of the Company;
- identification of security threats of PD during their processing in PDIS;
- application of organizational and technical measures to ensure the PD Security when Processing PD in PDIS, necessary to meet the requirements for the protection of PD, the implementation of which ensures the levels of PD protection established by the Decree of the Government of the Russian Federation No. 1119;
- application of the Information Security Systems conformity assessment that have been carried out in accordance with the established procedure;
- evaluation of the effectiveness of the measures taken to ensure the PD Security before the commissioning of PDIS;
- record-keeping of Company employees allowed to process;
- record-keeping of material Carriers of PD;
- detection of facts of unauthorized access to PD and taking measures;
- restoration of PD modified or destroyed as a result of unauthorized access to them;
- establishment of rules for access to PD processed in PDIS, as well as ensuring registration and recording of all actions performed with PD in PDIS;

- control over the measures taken to ensure the PD Security and the level of protection of PDIS;
- determination of the procedure for assigning information systems to personal data information systems based on approved criteria;
- determination of PD protection level for each PDIS;
- implementation of identification and authentication systems in each PDIS, access rights differentiation and registration of PDIS user actions;
- implementation of the information backup system for each PDIS;
- application of anti-virus protection systems and firewalls to protect PDIS.

A range of measures stipulated by the Decree of the Government of the Russian Federation No. 1119 and the Order of the FSTEC of Russia dated 02/18/2013 No. 21 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems", in order to ensure the PD Security in the Company is determined in the internal regulations of the Company, taking into account the results of the assessment of possible harm to PD Subject, which can be inflicted in the event of a violation of his PD Security, the relevance of threats to PD Security, as well as establishing the level of protection of PD.

11. Control over compliance with the legislation of the Russian Federation and the Company’s internal regulations in the field of PD

Internal control over the Company's compliance with the requirements of the legislation of the Russian Federation and the Company's internal regulatory documents in the field of PD shall be carried out by the Person Responsible for organizing the PD processing on an ongoing basis with the involvement of the Person Responsible for PD Security.

The Person Responsible for the organization of PD processing, in particular, is obliged to:

- exercise internal control over compliance by the Company and the Company's Employees with the legislation of the Russian Federation on PD, including the requirements for personal data protection;
- inform the Company's employees about the provisions of the legislation of the Russian Federation on PD, internal regulatory documents of the Company on PD processing, requirements for PD protection;
- organize receiving and processing of appeals and requests of PD Subjects or their representatives and (or) to monitor the receiving and processing of such appeals and requests.

12. PD Breach response procedure

An employee of the Company is obliged to immediately notify the Person Responsible for PD Security about the fact of a PD leak that has become known to him, is being prepared or has happened, using corporate email or corporate phone.

The notification of a PD leak shall contain information about the source of the information, the date and time of the event, information about the categories of PD and PD information systems from which the PD leak occurred and other circumstances known to the employee.

The Person Responsible for PD Security shall immediately carry out a preliminary analysis of the circumstances reported by the employee and, if the fact of leak is confirmed, shall immediately:

- inform the management of the Company about the fact;
- initiate an inspection with the involvement of interested division of the Company;
- identify the alleged causes of PD leak;
- assess the alleged harm caused to the rights of PD Subjects.

No later than 24 hours after the detection of a PD leak, the Person Responsible for PD Security notifies Roskomnadzor of the alleged causes led to the violation of PD subject rights and the alleged harm caused to PD subject rights, of the measures taken to eliminate the consequences of PD leak, and also provides information about the person authorized by the Company to interact with Roskomnadzor on issues related to the revealed fact of PD leak.

According to the results of the inspection on the PD leak, the Person Responsible for PD Security no later than 72 hours from the moment of detection of the PD leak shall notify Roskomnadzor about the results of the inspection, as well as provide information about the persons whose actions caused it (if any).

13. Responsibility for implementing the provisions of the Policy

Company employees who process personal data, as well as Person Responsible for PD Processing and Person Responsible for PD Security bear disciplinary, civil, administrative or criminal liability in accordance with the legislation of the Russian Federation for violation of the requirements of this Policy and other internal regulations of the Company in the field of PD and legislation of the Russian Federation in the field of PD.