

APPROVED

Director General

(position)

A.V. Dyukov

(signature)

(name)

« ____ » 20 September 2017 17:50:05



ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «ГАЗПРОМ НЕФТЬ»
(ОАО «ГАЗПРОМ НЕФТЬ»)

Policy

Policy for the Handling of Personal Data

Policy information

- 1 1 PREPARED by Corporate Security Department
- 2 2 PROCESS OWNER: Head of Information Security Office for Corporate Security Department
- 3 This document was developed under the Standardization Plan for 2015.
- 4 REVISION 1.0 INTRODUCED FOR THE FIRST TIME

Introduction

This policy for the handling of personal data is designed to ensure compliance by JSC Gazprom Neft with the laws of the Russian Federation and takes into account the requirements of the Constitution of the Russian Federation, legislative and other regulatory legal acts of the Russian Federation in the sphere of personal data.

1 Scope

1.1 The policy for the handling of personal data (“the Policy”) by JSC Gazprom Neft (“the Company”) defines the main principles, goals, conditions and methods for handling personal data, as well as lists of subjects of personal data and of the types of personal data, which are handled by the Company, together with the functions of the Company in handling personal data, the rights of subjects of personal data, and the requirements for the protection of personal data, which are implemented by the Company.

1.2 The provisions of the Policy are to be used for the design of local regulations governing issues related to the handling of personal data of Company employees and other subjects of personal data.

1.3 The Policy is recommended for adaptation and use by Company subsidiaries.

1.4 Terms and abbreviations used throughout this Policy are given in Annex 1.

2 2 Laws and other regulatory legal acts of the Russian Federation, which are used as guidance for the Policy

2.1 The following regulatory legal acts have been used as guidance in preparing this Policy:

- The Labour Code of the Russian Federation;
- Federal Law No. 152-FZ "On Personal Data", dated 27 July, 2006;
- Decree of the President of the Russian Federation No. 188 "On Approving the List of Confidential Information", dated 6 March, 1997;
- Resolution of the Government of the Russian Federation No. 687 "On approval of the Regulations on specifics of the handling of personal data without the use of automation", dated 15 September, 2008;
- Resolution of the Government of the Russian Federation No. 512 "On approval of requirements for physical bearers of biometric personal data and technologies for storing such data outside personal data information systems", dated 6 July, 2008;
- Decree of the Government of the Russian Federation No. 1119 "On approval of requirements for the protection of personal data during their processing in personal data information systems", dated 1 November, 2012;
- Order of the Federal Service for Technical and Export Control No. 21 "On approval of the composition and content of organizational and technical measures to ensure the safekeeping of personal data during their processing in personal data information systems", dated 18 February, 2013,
- Order of Roskomnadzor No. 996 "On approval of requirements and methods for the depersonalization of personal data", dated 5 September, 2013;
- other regulatory legal acts of the Russian Federation and regulatory documents of authorized state bodies.

3 Principles and goals of the handling of personal data

3.1 The Company, in its operations with personal data, handles the personal data of its

employees and other subjects of personal data, who are not in labour relationships with the Company.

3.2 In its handling of personal data the Company takes account of the need to protect the rights and freedoms of Company employees and other subjects of personal data, including protection of the right to privacy and the non-disclosure of personal and family matters, based on the following principles:

- the handling of personal data by the Company is carried out on a law-based and equitable basis;
- the handling of personal data is limited to the achievement of specific, pre-defined and legitimate purposes;
- it is not permitted to handle personal data in a manner incompatible with the purposes, for which it was collected;
- it is not permitted to combine databases containing personal data, when the goals of handling of the data in the respective databases are incompatible with one another;
- handling of personal data should be limited to data, which match the purposes of such handling;
- the content and volume of personal data, which are handled, should be consistent with the declared purposes of their handling. It is not permitted to handle an amount of personal data, which is excessive in comparison with the stated purposes of their handling;
- when handling personal data, their accuracy, sufficiency, and, if necessary, their relevance for the purposes of such handling should be ensured. The Company takes the necessary measures or ensures that measures are taken to delete or clarify incomplete or inaccurate personal data;
- personal data should be stored in a form, which does not allow identification of the subject of the personal data for longer than is required by the purpose of its handling, unless the period of storage of the personal data is regulated by federal law or by a contract, to which the subject of the personal data is a party, beneficiary or guarantor;
- the personal data, which is handled, should be destroyed or depersonalized upon the achievement of the purposes of its handling or in case the achievement of those purposes is no longer required, unless otherwise provided by federal law.

3.3 Handling of personal data is carried out by the Company for the following purposes:

- to ensure compliance with the Constitution of the Russian Federation, laws and other regulatory legal acts of the Russian Federation, and local regulations of the Company;
- exercise of the functions, powers and duties imposed on the Company by the laws of the Russian Federation, including the provision of personal data to state bodies, the Pension Fund of the Russian Federation, the Social Insurance Fund of the Russian Federation, the Federal Compulsory Medical Insurance Fund, and other state bodies;
- regulation of labour relations with employees of the Company (assistance in finding employment, training and promotion, personal security, monitoring of the quantity and quality of work carried out, ensuring the safekeeping of property);
- provision of additional guarantees and compensations to Company employees and members of their families, including non-state pension provision, voluntary medical insurance, medical services and other types of social security;
- protection of the life, health or other vital interests of the subjects of personal data;

- preparation, signing, execution and termination of contracts with counterparties;
- provision of the access and intrasite security at Company facilities;
- preparation of reference materials for internal information support of the Company, its subsidiaries, JSC Gazprom, its branches and representative offices, as well as subsidiaries and organizations of JSC Gazprom;
- execution of court orders, orders of other bodies or officials, which are subject to execution under the laws of the Russian Federation on enforcement proceedings;
- implementation of the rights and legitimate interests of the Company in the conduct of activities specified in the Charter and other local regulatory acts of the Company, or of third parties, or for the achievement of socially significant purposes;
- other legitimate purposes.

4 List of subjects, whose personal data are handled by JSC Gazprom Neft

The Company handles the personal data of the following groups of subjects:

- employees of the Company's business units;
- employees of the Company's subsidiaries;
- other subjects of personal data (to ensure implementation of the purposes of data handling, which are specified in Section 3 of this Policy).

5 List of personal data, which are handled by JSC Gazprom Neft

5.1 The list of personal data handled by the Company is determined by the laws of the Russian Federation and local regulations of the Company, taking account of the purposes of personal data handling, which are specified in Section 3 of this Policy.

5.2 The Company does not handle special categories of personal data, which concern race, nationality, political views, religious or philosophical beliefs, and private life.

6 The functions of JSC Gazprom Neft in the handling of personal data

6.1 When handling personal data the Company:

- takes necessary and sufficient steps to ensure compliance with the requirements of the laws of the Russian Federation and local regulations of the Company regarding personal data;
- takes legal, organizational and technical measures to protect personal data from unauthorized or accidental access, destruction, modification, blockage, copying, provision to third parties and dissemination, and from other illegal actions in respect of personal data;
- appoints a person to be responsible for management of the handling of personal data by the Company;
- publishes local regulations regarding the Policy and regarding the management and protection of personal data by the Company;
- acquaints employees of the Company who are directly involved in the handling of personal data with the provisions of Russian law and local regulations of the Company regarding personal data, including requirements for the protection of personal data, and ensures proper training of those employees;
- publishes or otherwise provides unrestricted access to this Policy;
- informs the subjects of personal data or their representatives concerning the availability of the personal data of such subjects, and enables them to acquaint

themselves with such personal data at their request and (or) upon their application or that of their representatives, unless otherwise provided by the laws of the Russian Federation;

- terminates the handling of personal data and destroys personal data in instances provided by the laws of the Russian Federation regarding personal data;
- carries out other actions provided by the laws of the Russian Federation regarding personal data.

7 Conditions for the handling of personal data by JSC Gazprom Neft

7.1 The Company handles personal data with the consent of the subject of the personal data, unless otherwise provided by the laws of the Russian Federation regarding personal data.

7.2 The Company does not disclose personal data to third parties and does not distribute personal data without the consent of the subject of those data, unless otherwise provided by federal law.

7.3 The Company has the right to entrust the handling of personal data to another person with the consent of the subject of the personal data on the basis of a contract made with that person. The contract should contain a list of actions (operations) with the personal data, which will be performed by the person handling them, the purpose of the handling, the duty of such person to respect the confidentiality of the personal data and to ensure their safety during handling, as well as requirements for protection of personal data, which are provided under Article 19 of the Federal Law "On Personal Data".

7.4 The Company may, for the purposes of internal information support and with the written consent of the subject of personal information, create internal reference materials, which contain the family name, first name, patronymic, place of work, position, year and place of birth, address, subscriber number, email address and other personal information, which has been communicated by that subject, unless otherwise provided by the laws of the Russian Federation.

7.5 Access to personal data handled by the Company is only permitted to employees holding positions, which are included in the Company's list of positions that involve the handling of personal data (except for publicly available and (or) depersonalised data).

8 List of actions with personal data and ways of handling personal data

8.1 The Company collects, records, systemizes, accumulates, stores, clarifies (updates, modifies), retrieves, uses, transfers (distributes, provides, gives access to), depersonalizes, blocks, deletes and destroys personal data.

8.2 The Company handles personal data in the following ways:

- manual handling of personal data;
- automated handling of personal data with or without the transfer of information, which has been received, through IT and telecommunications networks;
- mixed handling of personal data.

9 Rights of the subjects of personal data

9.1 The subjects of personal data have the right to:

- receive full information about their personal data, which are handled by the Company;
- access their personal data, including the right to receive a copy of any record

containing their personal data, except as provided by federal law, as well as access to medical data concerning them, with the help of a medical specialist of their choice;

- clarify their personal data, and block or destroy the data in case they are incomplete, outdated, inaccurate, obtained illegally or are not necessary for the declared purpose of their handling;
- withdraw consent to the handling of personal data;
- take steps provided by law for the protection of their rights;
- appeal to the authorized body for the protection of the rights of subjects of personal data or to a court against any action or inaction of the Company, which breaches provisions of the laws of the Russian Federation regarding personal data;
- exercise other rights provided by the laws of the Russian Federation.

10 Steps taken by PJSC Gazprom Neft to ensure the performance of its duties during the handling of personal data

10.1 The following steps are necessary and sufficient to ensure the Company's performance of its duties provided by the laws of the Russian Federation regarding personal data:

- approval of local regulations and other documents regarding the handling and protection of personal data;
- training and methodological work with employees at Company business units whose job definitions include the handling of personal data;
- obtaining the consent of subjects of personal data to the handling of their personal data, except for cases provided by the laws of the Russian Federation;
- separating personal data, which are handled without the use of automation, from other information, specifically by storing them on separate physical bearers and in special sections;
- ensuring separate storage of personal data, which are handled for different purposes and which contain different data categories, and separate storage of their physical bearers;
- prohibiting the transfer of personal data through open-access communication channels, computer networks outside a controlled zone, the corporate data transmission network of PJSC Gazprom Neft, the Gazprom Unified Data Transmission Network and internet networks without the use of measures established in the Company to ensure the security of personal data (except for publicly available and (or) depersonalised personal data);
- storage of physical bearers of personal data in compliance with conditions designed to ensure the safekeeping of personal data and to prevent unauthorized access to them;
- internal monitoring to ensure that personal data handling complies with the Federal Law "On Personal Data" and regulatory legal acts adopted in accordance with that Law, and also with requirements for the protection of personal data, this Policy, and local regulations of the Company;
- other measures provided by the laws of the Russian Federation regarding personal data.

10.2 Measures to ensure the safekeeping of personal data during their handling in personal data information systems are established by the Company's local regulations, which regulate the safekeeping of personal data during their handling in the Company's personal data information systems.

11 Monitoring of compliance with the laws of the Russian Federation and local regulations of JSC Gazprom Neft regarding personal data, including requirements for the protection of personal data

11.1 The management and internal monitoring of observance by Company business units of the laws of the Russian Federation and local regulations regarding personal data, including requirements for the protection of personal data, are to be carried out by the person responsible for management of the handling of personal data by the Company.

11.2 Internal monitoring of the compliance of personal data handling with the Federal Law "On Personal Data" and related regulatory legal acts, and also with personal data protection requirements, this Policy and local regulations of the Company is the responsibility of the Directorate for Corporate Protection.

11.3 Heads of the Company's business units bear personal responsibility for compliance of those business units with the requirements of the laws of the Russian Federation and local regulations of the Company regarding personal data, and for ensuring the confidentiality and safekeeping of personal data at Company business units.

12 Documentary and information support for the implementation of this Policy

Appropriate local regulations and other documents should be prepared in order to implement the provisions of this Policy by the Company, including:

- Regulations on the handling of personal data;
- Regulations on ensuring the safekeeping of personal data during their handling in personal data information systems;
- a list of jobs, which include in their description the handling of personal data;
- rules for the handling of personal data by Company business units;
- other local regulations and documents, which regulate matters connected with the handling of personal data by the Company.

Appendix 1 Terms and Definitions

The following terms and definitions are used in this Policy.

Personal data any information related to a person who is directly or indirectly specified or in the process of being specified (a subject of personal data).

Information: information (communications, data), in whatever form.

Operator: a state body, municipal body, legal entity or individual, which independently or jointly with other entities/persons manages and (or) carries out the handling of personal data, and defines the purposes of personal data handling, the nature of the personal data to be handled, and the actions (operations) that are carried out with personal data.

Personal data handling: any action (operation) or set of actions (operations) performed with personal data, either with or without the use of automation tools, including collection, recording, systematization, accumulation, storage, clarification (updating, modification), extraction, use, transfer (distribution, provision, giving access to), depersonalization, blocking, deletion and destruction of personal data.

Automated handling of personal data: Handling of personal data with the use of computer equipment.

Provision of personal data: actions for the disclosure of personal data to a specific person or a specific circle of persons.

Dissemination of personal data: actions for the disclosure of personal data to an indeterminate circle of persons.

Blocking of personal data: temporary suspension of the handling of personal data (except for cases when handling is necessary in order to verify personal data).

Destruction of personal data: actions, as a result of which it becomes impossible to restore the content of personal data in a personal data information system and (or) as a result of which physical bearers of personal data are destroyed.

Depersonalization of personal data: actions, as a result of which it becomes impossible, without additional information, to determine the reference of personal data to a specific subject of personal data.

Personal data information system: a totality of personal data contained in databases and the information technologies and technical equipment, which enable handling of the personal data.