


APPROVED
by Order of PJSC “Rostelecom”
No01/01/1150-15 dated 24.12.2015

Personal Data Processing Policy of PJSC Rostelecom
(Version 1)
(with amendments from 14.02.2020)

Moscow
2015

Table of Content

1	THE PURPOSE	3
2	GENERAL.....	3
2.1	SCOPE	3
2.2	TERMS, DEFINITIONS AND ABBREVIATIONS	3
2.3	REFERENCES	4
3	CATEGORIES OF PERSONAL DATA SUBJECTS	5
4	PURPOSES OF PERSONAL DATA PROCESSING	5
5	PRINCIPLES OF PERSONAL DATA PROCESSING.....	6
6	RIGHTS OF PERSONAL DATA SUBJECTS	7
7	PERSONAL DATA CONFIDENTIALITY	8
8	PERSONAL DATA PROCESSING PERIOD	8
9	TRANSFER OF PERSONAL DATA	8
10	ENSURING PERSONAL DATA SECURITY.....	8
11	IMPLEMENTING COMPLIANCE WITH PERSONAL DATA PROTECTION REQUIREMENTS.....	9
12	PERSONAL DATA DESTRUCTION (DEPERSONALIZATION).....	9
13	LIABILITY FOR VIOLATION OF PROVISIONS REGULATING PERSONAL DATA PROCESSING.....	10
14	STORAGE AND ARCHIVING.....	11
15	DISTRIBUTION AND UPDATES.....	11

 Rostelecom	Personal Data Processing Policy	
Version: 1/2015	Business Process: P14	Page 3 of 11

1 The Purpose

This Personal Data Processing Policy as applied at PJSC Rostelecom (the “Policy”) shall set forth requirements applicable to the personal data processing framework.

Personal data processing, scope and volume of the processed personal data are determined according to the Russian Constitution, Federal Russian law No 152-FZ of 27.07.2006 “On Personal Data”, other federal laws and statutory regulations.

This Policy is introduced for the first time and takes effect as of the date of its approval.

2 General

2.1 Scope

This Policy is publicly accessible and shall be made available at the Company information boards and posted on the website at www.rt.ru.

Requirements of this Policy shall be applicable to all Employees of Rostelecom.

Application of this Policy in the Company Macroregional/Regional Branches, General Service Center and Training and Production Center: for guidance.

2.2 Terms, definitions and abbreviations

For the purposes of this Policy, terms and acronyms defined in Rostelecom glossary of terms and definitions, as well as the following terms are used:

Subscriber shall mean a user of communication services with whom an agreement for the provision of such services was made with allocation of a subscriber number or unique identification code for these purposes.

Personal data shall mean any information related to a directly or indirectly identified or ascertained individual (personal data subject).


Personal data depersonalization (anonymization) shall mean making it impossible to identify the specific personal data subject without using additional information.

Personal data processing shall mean implementation of any action (operation) or a consistent set of actions (operations) performed with personal data using automation tools or without using such tools, including collection, recording, systematization, accumulation, storage, refinement (update, change), retrieval, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of personal data.

The Company shall mean Public Joint Stock Company “Rostelecom” (hereinafter “Rostelecom”).

Visitor shall mean an individual who is not an employee of the Company, but is temporarily located on its territory or premises.

Provision of personal data shall mean actions aimed at disclosing personal data to a certain person or a specific group of persons.

 Rostelecom	Personal Data Processing Policy	
Version: 1/2015	Business Process: P14	Page 4 of 11

Employee shall mean an individual who entered into an employment relationship with Rostelecom.

Personal data dissemination shall mean actions aimed at disclosing personal data to an indefinite number of persons.

Personal data subject (Subject of personal data) shall mean an individual to whom the relevant personal data relates.

Personal data destruction shall mean implementing actions making it impossible to recover the content of personal data in the personal data information system and/or destruction of tangible media containing personal data.

DCIS shall mean Department of Corporate Information Security of Rostelecom.


PJSC shall mean public joint stock company.

FSTEC shall mean the Federal Service for Technical and Export control.

2.3 *References*

This Policy was developed using the following legal documents:

- The Constitution of the Russian Federation as of 12.12.1993;
- Russian Labor Code as of 30.12.2001 No 197-FZ;
- Russian Federal Law No 152-FZ of 27.07.2006 “On Personal Data”;
- Russian Federal Law No 149-FZ of 27.07.2006 “On information, information technologies and information protection”;
- Decree of the Russian President No 188 of 06.03.1997 “Approval of the list of confidential information items”;
- The Russian Government resolution No 512 of 06.07.2008 “On approval of requirements to be complied with by biometric personal data media and technologies of storage of such data outside any personal data information systems”;
- The Russian Government resolution No 538 of 27.08.2005 “Approval of the Rules of interaction between telecommunications operators and state authorities performing search and criminal investigation activities”;
- The Russian Government resolution No 1119 of 01.11.2012 “Approval of personal data protection requirements in the course of personal data processing in personal data information systems”;
- The Russian Government resolution No 687 of 15.09.2008 “Approval of Regulations on specifics of personal data processing without use of automation tools”;
- The Russian Government resolution No 1342 of 09.12.2014 “Procedure of telephone service provision”;
- Order of the Russian FSTEC No 21 of 18.02.2013 “Approval of the list and content of organizational and technical measures to ensure personal data security in the course of persona; data protection in the personal data information systems”;

 Rostelecom	Personal Data Processing Policy	
Version: 1/2015	Business Process: P14	Page 5 of 11

- [Rostelecom Information Security Policy](#);
- [Regulations on processing and protection of Rostelecom employees' personal data](#);
- [Cryptographic protection usage policy of Rostelecom](#);
- [Rostelecom file management guidelines](#);
- [Procedure of drafting, designing and approval of drafts of direction documents \(orders, instructions\) in Rostelecom, using e-document flow system \(ESED\)](#).

3 Categories of personal data subjects


Personal data of the following personal data subject categories shall be processed in the Company:

- Employees of the Company;
- Candidates for vacant positions;
- Persons accepted for internship;
- Dismissed former employees;
- Relatives of employees;
- Subscribers and persons intending to make a communication services contract with the Company (potential subscribers);
- Shareholders of the Company and members of the Board of Directors;
- Persons with whom contracts under the civil law were concluded;
- Visitors of the Company;
- Representatives of the Company's counterparties, including contact persons of the counterparties; Representatives of personal data subjects authorized to represent their interests.

4 Purposes of personal data processing

Personal data shall be processed in Rostelecom for the following purposes:

- Personal data of the Company's employees is processed to ensure compliance with laws and other statutory regulations, facilitate employees' employment, their education and promotion, ensure employees' personal safety, monitor the volume and quality of work performed and ensure the safeguarding of property, ensure compliance with the legislation of the Russian Federation, facilitate employment, training and promotion of employees, control of the quantity and quality of work performed, for ensuring the safety of property, ensuring compliance with access rules and internal rules and regulations effective on the Company premises.
- Personal data of candidates for vacant positions is processed to ensure compliance with the laws of the Russian Federation and other statutory regulations, facilitate employment, verify business and personal qualities, ensure compliance with access rules and internal rules and regulations effective on the Company premises.
- Personal data of persons accepted for internship shall be processed to ensure compliance with the laws of the Russian Federation and other statutory regulations,

 Rostelecom	Personal Data Processing Policy	
Version: 1/2015	Business Process: P14	Page 6 of 11

facilitate training and employment, ensure compliance with access rules and internal regulations effective on the Company premises.


- Personal data of dismissed former employees is processed to ensure compliance with the laws of the Russian Federation and other statutory regulations, including those applicable to accounting and tax accounting, to ensure archival storage of documents, provide guarantees and compensations established by the current legislation and internal regulations of the Company, ensure compliance with access rules and internal rules and regulations effective on the Company premises.
- Personal data of employees' relatives is processed to ensure compliance with the laws of the Russian Federation and other statutory regulations, to provide guarantees and compensations to employees of the Company established by the current legislation and internal regulations of the Company;
- Personal data of subscribers shall be processed for the purpose of fulfilment of communications service provision contracts concluded between the Company and the relevant subscriber. Personal data of persons wishing to conclude communication service agreement with the Company (potential subscribers) is processed in order to conclude a communication service provision agreement by the Company with a potential subscriber.
- Personal data of the Company shareholders and members of the Board of Directors shall be processed in order to ensure compliance with the laws of the Russian Federation and other statutory regulations, observance of the rights and legitimate interests of the Company shareholders and members of the Board of Directors, ensure mandatory information disclosures and making dividend payments to shareholders, and pay remunerations to members of the Board of Directors;
- Personal data of the Company's visitors shall be processed in order to ensure compliance with access rules and internal regulations effective on the employer's premises;
- Personal data of representatives of the Company's counterparties, including contact persons of such counterparties shall be processed for the purpose of performance under the concluded contracts.
- Personal data of representatives of the personal data subjects shall be processed in order to ensure observance of the rights and legitimate interests of the personal data subject, who authorized the relevant representative to represent the personal data subject's interests within the framework of relationship with the Company.

5 Principles of Personal data processing

Personal data shall be processed lawfully and on a fair basis.

The scope of the personal data processing shall be limited to achieving specific, predetermined and legal purposes. No personal data processing that is inconsistent with the purposes of collecting personal data shall be allowed.

It is not allowed to merge any databases containing personal data, where the purposes of such personal data processing are inconsistent with each other.

 Rostelecom	Personal Data Processing Policy	
Version: 1/2015	Business Process: P14	Page 7 of 11

Only the personal data that meets the purposes of its processing shall be subject to processing.

The content and volume of the processed personal data must be consistent with the stated purposes of the processing. The processed personal data should not be excessive in relation to the stated purposes of the processing.

Accuracy and sufficiency of the personal data, and, if necessary, relevance to the purposes of the personal data processing must be ensured in the course of the personal data processing. The operator must either take necessary measures or ensure that such measures are taken in order to remove or rectify any incomplete or inaccurate data.

Personal data processing can be implemented both using automation tools and without using such tools.


Storage of any personal data in a form that makes it possible to identify the relevant personal data subject shall be allowed only for a period, not longer than it is required for the purposes of personal data processing, unless the duration of the personal data storage is prescribed by applicable federal law.

The processed personal data shall be destroyed or depersonalized upon achievement of the processing purposes, or where achievement of such purposes is no longer needed, unless otherwise is provided by federal law.

6 Rights of personal data subjects

Subjects whose personal data is processed in the Company shall have the right to receive information regarding personal data processed by the Company within the framework and in the scope prescribed in the Federal Russian Law "On Personal Data", as well as the following rights:

- to receive complete information about their personal data;
- to be provided with free of charge readily available access to their personal data, including the right to receive free copies of any record containing personal data of the relevant subject. Information about the availability of personal data must be provided to the personal data subject in an accessible form, and should not contain any personal data related to other personal data subjects. Access to the subject's personal data shall be provided by the Company to the personal data subject in question or his/her representative upon personal contact, or upon receipt of a request;
- to receive information about the Company, its location, availability from Company of any information about personal data related to the relevant personal data subject;
- to request that the Company should rectify, delete or amend any incomplete, incorrect, outdated, inaccurate, illegally obtained personal data, or personal data not required for the stated purpose of its processing, as well as to take measures afforded by law to protect rights of the personal data subjects;
- to request that the Company should notify all persons who were previously provided with incorrect or incomplete personal data, about all deletions in, corrections of or additions to such personal data;

 Rostelecom	Personal Data Processing Policy	
Version: 1/2015	Business Process: P14	Page 8 of 11

- to appeal to the authorized body for the protection of rights of personal data subjects or in court against any unlawful actions or inaction of the Company committed in the course of processing and protecting his/her personal data.

7 Personal data confidentiality

The Company and other persons who obtained access to personal data shall be obliged not to disclose to third parties, nor to distribute personal data without consent of the relevant personal data subject, except as otherwise provided by applicable law.

8 Personal data processing period

The term of processing of the personal data processed in the Company is determined pursuant to internal administrative and organizational regulations of the Company in accordance with provisions of the Federal Russian Law "On Personal Data".

The duration of personal data processing periods is determined in accordance with the effective term of the agreement with the relevant personal data subject, pursuant to Order of the Russian Ministry of Culture No 558 of 25.08.2010 "Approval of the List of standard administrative management archived documents generated in the course of activities performed by state bodies, local municipal governments and organizations, specifying the storage periods", subject to limitation periods, as well as other periods set forth by applicable Russian law and internal organizational and administrative documents of the Company.

Any personal data with expired term of its processing, shall be destroyed, unless otherwise is provided by applicable federal law.


9 Transfer of personal data

In the course of pursuing its activities the Company may provide some subjects' personal data to third parties in accordance with requirements of applicable Russian law or upon consent of the relevant personal data subject, always provided, that undertaking by the parties involved of obligations to maintain confidentiality and ensure security of the personal data in the course of its processing should be a mandatory condition for provision of any personal data to a third party.

10 Ensuring personal data security

Rostelecom takes any necessary organizational and technical measures to ensure security of personal data to prevent any accidental or unauthorized access, destruction, alteration, blocking of access and other unauthorized actions in respect of personal data.

Personal data obtained by Rostelecom for legitimate purposes will not be disseminated, nor provided to third parties without consent of the relevant personal data subject, unless otherwise is provided by applicable federal law.

 Rostelecom	Personal Data Processing Policy	
Version: 1/2015	Business Process: P14	Page 9 of 11

11 Implementing compliance with personal data protection requirements

Rostelecom maintains compliance with the following personal data requirements of applicable law:

- requirements to honor personal data confidentiality;
- requirements to ensure the ability of personal data subject to exercise his/her rights;
- requirements to ensure the accuracy of personal data, and, if necessary, the updated status in respect of the purposes of personal data processing (with implementation (ensuring implementation) of measures to delete/destroy or rectify incomplete or inaccurate data);
- requirements for personal data protection from unauthorized or accidental access to such data, and against destruction, modification, blocking, copying, provision, dissemination of personal data, as well as from other illegal actions in connection with personal data;
- other applicable law requirements.


Pursuant to the Russian Federal Law No 152-FZ of 27 July 2006 “On Personal data” Rostelecom shall independently identify the list and scope of measures that are necessary and sufficient for compliance with duties prescribed by applicable personal data law.

In particular, personal data security is achieved by the following:

- appointing a person responsible for personal data processing and protection;
- issuing this Policy;
- issuing local internal regulations on matters related to personal data processing;
- making employees who are allowed to process subjects’ personal data aware of requirements of applicable Russian law on personal data, this Policy and internal Rostelecom rules and regulations;
- implementing proper arrangements of personal data treatment, where automation tools are used (including, but not limited to, using certified software, delimitation of access to computers, LAN, IT systems where personal data is processed, establishing a procedure of elimination of personal data residing in IT systems);
- implementing proper arrangements of personal data treatment where no automation tools are used (including, but not limited to, proper storage of documents containing personal data, implementation of the procedure to destroy/depersonalize personal data processed without using automation tools);
- establishing a procedure of employees’ access to information containing any personal data of personal data subjects according to such employees’ job (functional) duties;
- exercising internal control over and/or audits of the compliance of personal data processing with the federal law and regulations adopted in accordance with them, with requirements for personal data protection, the operator's policy of personal data processing and the operator’s internal rules.

12 Personal data destruction (depersonalization)

Subject’s personal data shall be destroyed (depersonalized) in the following cases:

 Rostelecom	Personal Data Processing Policy	
Version: 1/2015	Business Process: P14	Page 10 of 11


- within not more than thirty days after the personal data processing purposes are achieved or if achievement of such purposes is no longer needed, unless otherwise is provided by the contract, where the personal data subject is a the party to, beneficiary or surety under such contract, or according to other agreement between the Company and the personal data subject, or according to relevant provisions of Russian federal laws if the Company is not entitled to process personal data without the consent of the personal data subject;
- within not more ten (10) business days after detecting an instance of unlawful personal data processing by the Company, if such unlawful personal data processing is found;
- within not more than thirty (30) days after receipt from the personal data subject of a notice of revocation of his/her consent to processing his/her personal data, where further storage of personal data is no longer needed for the purposes of the personal data processing by the Company, unless otherwise is provided by the contract, where the personal data subject is a the party to, beneficiary or surety under such contract, or according to other agreement between the Company and the personal data subject, or according to relevant provisions of Russian federal laws if the Company is not entitled to process personal data without the consent of the personal data subject;
- if the personal data storage period, determined in accordance with applicable Russian law and organizational and administrative documents of the Company is expired;
- if a relevant order of the authorized body for protection of rights of personal data subjects, the Prosecutor's Office of Russia is issued or a court decision is handed over.

In the event of inconsistency of the purposes of processing of personal data, residing on a tangible media, if such media does not make it possible to process personal data separately from other personal data residing on the same medium, and if it is required to destroy or block part of personal data, the tangible media should be destroyed or blocked subject to prior copying of information that should not be destructed or blocked, using a method that prevent any simultaneous copying of personal data to be destructed or blocked.

A part of personal data can be destructed, if the relevant tangible media makes it possible, using a method (deletion, erasing) that prevents any further processing of such personal data while preserving the possibility of processing other data recorded on the tangible media.

13 Liability for violation of provisions regulating personal data processing

The Company and/or its Employees found guilty of violation of requirements of applicable Russian law on personal data or provisions of this Policy shall be held liable according to applicable Russian law.

 Rostelecom	Personal Data Processing Policy	
Version: 1/2015	Business Process: P14	Page 11 of 11

14 Storage and archiving

The original counterpart of this Policy should be kept by Division of Documentary Support and Archiving of General Affair Management Department according to requirements of Rostelecom File Management Guidelines.

15 Distribution and updates

This Policy should be revised and updated by Rostelecom’s Corporate Information Security Department from time to time as required, but at least once every 24 months.

The decision to initiate the process of making amendments to the document shall be made by the Director of the Corporate Information Security Department based on proposals from other divisions, results of the document use in Rostelecom, analysis of recorded and corrected inconsistencies, as well as following recommendations of internal or external audits.

The procedure for regular inspections and making changes to the Policy is defined in the File Management Guidelines in Rostelecom.

The current version of the approved Policy should be posted on the Intranet portal in the Company's IRR Register on the page of Corporate Information Security Department indicating the Policy belonging to P14 “Security” business process.

Director of Corporate Information Security Department is responsible for initiating the posting and keeping current the version of the Policy posted on the Intranet portal, as well as for making all stakeholders aware of the location of the current version of the Policy.