Sberbank of Russia

APPROVED
by Resolution of the Executive
Board of Sberbank
Minutes No. 506 dated 29 April 2014, § 27

29 April 2014 **No. 3324**

POLICY
on Personal Data Processing at Sberbank
(as amended under No.1 dated 17/11/2016, No.2 dated 4/07/2017, No.3 dated 28/12/2017)

Moscow,
2018

IRD details

IRD Name and Number	Policy on Personal Data Processing at Sberbank No. 3324
Unit responsible for IRD development	Customer Relations and Secondary Sales Development Department
IRD implemented by	Janette Levochkina, 36-532
IRD type / category	Core/Policy
Activity/Process code	0100 / not applicable

IRD applies to the following units	**[X]**	Central Head Office	**[X]**	Centrally Subordinated Units
	[X]	Regional banks	**[X]**	Internal structural units
	[X]	Branches	**[ ]**	Sberbank Group
	[X]	Branches abroad		

IRD for upper-level process	

IRD history

Version number	**Details of the administrative document approving this IRD / amendments to this IRD, date, and position of the approving officer**
1	Resolution of the Executive Board of Sberbank, Minutes No.506 dated 29/04/2014, §27 § 27
1/1	Resolution of the Executive Board of Sberbank, Minutes No. 554 dated 17/11/ 2016, §29a
1/2	Resolution of the Executive Board of Sberbank, Minutes No. 607 dated 4/04/2017, §1a
1/3	Resolution of the Executive Board of Sberbank, Minutes No. 624 dated 28/12/2017, §118a

IRDs ceasing to be effective after this IRD comes into force

IRD effective date	***IRD validity period***
Since the approval date	-

Information on crowdsourcing-driven expert review

TABLE OF

1. General Provisions

1.1. The Policy on Personal Data Processing at Sberbank (the "Policy") was developed in accordance with /1/, /2/, /3/, /4/, /5/, as well as with other federal laws and regulations of the Russian Federation that define the circumstances and specific features of personal data processing and maintaining the security and confidentiality of such information (the "Personal Data Legislation").

1.2. The Policy was developed for the purposes of implementing the requirements of legislation on processing and ensuring the security of personal data and is aimed at protecting human and civil rights and liberties when processing personal data at the Bank.

1.3. This Policy establishes:

- Objectives of personal data processing
- Classification of personal data and Personal Data Subjects
- General principles of personal data processing
- The principal participants of the personal data processing management system
- The main approaches to the personal data processing management system

1.4. The provisions of this Policy are the foundation for the system of personal data processing in the Bank, including for the development of 2nd- and 3rd-level internal regulatory documents (regulations, methodologies, flow charts, etc.) to govern personal data processing procedures at the Bank.

1.5. The provisions of this Policy shall be binding upon all Employees of the Bank who have access to personal data.

1.6. This Policy shall be published in a shared resource: Bank EDIRD (electronic database of internal regulatory documents) for general use by Bank Employees.

1.7. The Bank Employees shall be informed of the provisions of this Policy through the distribution of the Policy via the electronic document flow system used in the Bank.

2. Purposes of Personal Data Processing

2.1. The Bank shall process personal data for the following objectives:

- To conduct bank operations and transactions in accordance with the Charter of the Bank and licenses issued to the Bank for conducting banking and other operations
- To enter into any agreements with the Personal Data Subject and the further performance thereof
- To carry out promotions, surveys, and studies
- To provide information on services rendered by the Bank to the Personal Data Subject, on the development of new products and services by the Bank; on services of Bank subsidiary companies; and to inform the Client of product and service offers from the Bank
- To manage staff and organize record keeping on Bank Employees
- To attract and select Candidates for employment in the Bank
- To compile statistical reports, including that to be submitted to Bank of Russia
- To carry out administrative and maintenance activity by the Bank
- To regulate employment relations and directly related relations

- To detect fraud, stealing money from accounts and other unlawful acts, to prevent such unlawful acts in future and to localize any consequences of such acts;

To achieve the objectives provided for by any international treaty of the Russian Federation or law or for the implementation and performance of the functions, powers, and responsibilities with which the Bank is charged by Russian Federation law

3. Classification of Personal Data and Personal Data Subjects

3.1. Personal data means any information relating directly or indirectly to an identified or identifiable individual (Personal Data Subject), which is processed by the Bank to achieve predetermined objectives.

3.2. The Bank does not engage in the processing of special categories of personal data related to racial and ethnic identity, political views, religious and philosophical beliefs, intimate life, or the criminal record of individuals, unless otherwise established by the Russian law.

3.3. The Bank shall have the right to engage in the processing of special categories of personal data related to the health of the Personal Data Subject (insured persons and other persons in cases provided for by the current legislation).

The Bank shall have the right to engage in biometric personal data processing to identify customers and employees of the Bank at rendering banking services and establishing identity of customers and employees when granting the pass into the Bank.

3.4. The Bank shall process the personal data of the following categories of Personal Data Subjects:

- Individuals who are Candidates
- Individuals who are Bank Employees and their close relatives
- Individuals who provide services and have entered into a civil law contract with the Bank
- Individuals who are members of Bank management bodies
- Individuals who represent the interests of a Corporate Client of the Bank (Corporate Client Representatives)
- Individuals who are Retail Clients of the Bank
- Individuals who have purchased or intend to purchase Bank services or third-party services through the Bank or who do not have contractual relations with the Bank, provided that their personal data is included in the Bank's automated systems and processed in accordance with Personal Data Legislation
- Individuals who are not Bank Clients, who have entered into or intend to enter into contractual relations with the Bank in connection with administrative and maintenance activity performed by the Bank, provided that their personal data is included in the Bank's automated systems and processed in accordance with Personal Data Legislation
- Individuals who themselves make their personal data publicly available, provided that the processing thereof does not violate their rights and conforms to the requirements established by Personal Data Legislation
- Other individuals who have provided their consent to processing of their personal data by the Bank, or individuals whose personal data are required to be processed by the Bank for achieving the purposes contemplated by any international treaty

of the Russian Federation or law or for the implementation and performance of the functions, powers, and responsibilities with which the Bank is charged by Russian Federation law.

4. General principles of personal data processing

4.1. The Bank will process personal data on the basis of these general principles:

- The lawfulness of the predetermined, specific objectives and manner of personal data processing
- Ensuring proper personal data protection
- The conformity of the objectives for personal data processing to the objectives previously defined and announced during the collection of the personal data
- The conformity of the scope and nature of the personal data processed and the manner of its processing to the objectives of the personal data processing
- The accuracy of personal data, a sufficient amount of personal data for processing purposes, and the inadmissibility of more personal data processing than necessary for the objectives stated during the collection of the personal data
- The inadmissibility of combining databases containing personal data that is processed for mutually incompatible objectives
- The storage of personal data in a form permitting the Personal Data Subject to be identified for no longer than required by the processing objective
- The destruction or depersonalization of personal data after its processing objective is achieved, unless the period of personal data storage is established by the Russian law, a contract to or under which the Personal Data Subject is a party, beneficiary, or guarantor
- Maintaining the confidentiality and security of personal data to be processed

4.2. The following rights are established for the Personal Data Subject and the Bank with respect to personal data processing.

4.2.1. The Personal Data Subject shall have the right to:

- Retrieve information relating to the processing of their personal data according to the procedure and form and within the periods established by Personal Data Legislation
- Demand that their personal data be edited, Blocked, or Destroyed if their personal data is incomplete, outdated, inaccurate, illegally acquired, is not required for the stated objective of the processing, or is used for objectives not declared in advance when the Personal Data Subject provided their consent to the personal data processing
- Take measures for the protection of their rights provided for by law
- Revoke their consent to the personal data processing

4.2.2. The Bank shall have the right to:

- Process the personal data of the Personal Data Subject in accordance with the stated objective
- Demand that the Personal Data Subject provide the accurate personal data necessary to perform a contract, render a service, or identify the Personal Data Subject and in other cases provided for by Personal Data Legislation
- Limit the access of the Personal Data Subject to its personal data if Personal Data Processing is carried out according to the legislation on countering the legalization (laundering) of the proceeds

of crime and the financing of terrorism, the Personal Data Subject's access to its personal data violates rights and legal concerns of any third parties, as well in other cases specified by laws of the Russian Federation

- Process publicly available personal data of individuals
- Process personal data that is subject to publication or mandatory disclosure in accordance with the Russian law
- Assign the processing of personal data to another party with the consent of the Personal Data Subject

5. Principal participants of the personal data processing management system

5.1. The main participants of the personal data processing procedure shall be defined to ensure its effective management.

5.1.1. The Bank Executive Board shall:

- Define, review, and approve the Bank's policy on personal data processing.

5.1.2. Group Risks Committee of Sberbank shall:

- Make decisions on Bank actions related to the use of risk-prone personal data

5.1.3. The person responsible for organizing personal data processing and protection shall be appointed by the Order of CEO, Chairman of the Executive Board of Sberbank, and shall perform the following functions:

- Develop, organize and control the processing of personal data (carried out with the use of automation tools or without the use of such means, including on paper) in accordance with the Personal Data Law, this Policy, the Bank's internal regulations
- Provide management and constant improvement of personal data processing under the uniform rules, standardize and replicate the process
- Establish the composition of Key Performance Indicators (KPIs) for the process, develop methodologies to calculate and monitor KPIs and other indicators
- Develop the IRDs related to personal data processing issues, data protection requirements and submit them for approval to an appropriate joint authority of the Bank
- Organize communication and/or communicate to the Bank Employees the provisions of the Personal Data Legislation, this Policy, IRDs of the Bank regarding personal data processing, and personal data protection requirements
- Analyze, evaluate, and forecast risks associated with personal data processing at the Bank, develop risk mitigation measures
- Evaluate the impact of the Bank's processes on the rights and freedoms of Personal Data Subjects
- Analyze the automated systems and personal data processing processes to verify their compliance with the established mandatory requirements in the field of processing and protection of personal data
- Record the procedures and tools for personal data processing

- Control over existence and completeness of any personal data processing mandate agreement or personal data transfer agreement (DTA)
- Organize data exchange with European banks in accordance with /5/;
- Develop and organize the application of legal, organizational, and technical measures to prevent illegal or accidental access to personal data or the Destruction, Modification, Blocking, Copying, Provision, or Distribution of personal data, and other illegal acts with respect to personal data
- Identify threats to personal data security during processing
- Organize and supervise the level of security of personal data information systems
- Assess the effectiveness of measures taken to ensure personal data security
- Develop internal procedures aimed at personal data security and protection
- Organize and conduct internal control over the compliance of the processor and its employees with the Legislation on personal data, this Policy, IRDs of the Bank, personal data protection requirements
- Organize for the receipt and processing of appeals and requests from personal data subjects and their representatives, and (or) control the receipt and processing of such appeals and requests
- Provide methodological assistance to the Bank's structural units with regard to interaction with state and supervisory authorities engaged in data processing
- Interact with government authorities on personal data protection issues
- Notify any supervisory authority about personal data breaches in accordance with the applicable requirements
- Organize the notification of Personal Data Subjects about breaches of their personal data
- delegate[2] other functions provided by Personal Data Legislation for the party (parties) responsible for organizing personal data processing and protection to specialized business units of the Bank.

5.1.4. The Internal Audit Department shall:

- In the course of control procedures performed by it, assess the effectiveness of the internal oversight system at the Bank to ensure compliance with this Policy as well as with the approved regulatory documents of the Bank regarding personal data

5.1.5. The Legal Department shall:

- Monitor legislation and inform interested business units of changes to the law
- Represent the Bank's interests in court and to government authorities in disputes related to personal data processing as well as during the consideration of administrative cases related to a violation of the law in this area.

6. Organizing the personal data processing management system

6.1. Personal data of the Personal Data Subject shall be processed with their consent to the personal data processing and in the absence of such consent, if the Personal Data Processing is required for the performance of a contract, to or under which the Personal Data Subject is a party, beneficiary, or guarantor, as well as for the conclusion of a contract at the initiative of the Personal Data Subject, or a contract to or under which the Personal Data Subject will be a party, beneficiary, or guarantor, or in other cases provided for by Personal Data Legislation.

6.2. A special category of personal data related to the health of the Personal Data Subject shall be processed with the written consent of the Personal Data Subject to the personal data processing and in the absence of such consent, if the personal data is made publicly available by the Personal Data Subject.

6.3. The Bank has the right to assign the personal data processing to another party with the consent of the Personal Data Subject, unless otherwise provided by federal law. Such Personal Data Processing shall be done only on the basis of a contract executed between the Bank and the third party, which should define the following:

- The list of actions (operations) with personal data which will be done by the third party engaged in the personal data processing
- Objectives of personal data processing
- The obligations of the third party to maintain the confidentiality of personal data, to ensure its security during processing, and to comply with the requirements for the protection of the personal data being processed

6.4. The Bank shall provide personal data to public authorities pursuant to their powers in accordance with the Russian law.

6.5. The Bank shall be liable to the Personal Data Subject for the actions of the parties to whom the Bank assigns the personal data processing of the Personal Data Subject.

6.6. Access to the personal data being processed shall only be granted to those Bank Employees who require it to perform their official duties and in accordance with the principles of personal responsibility.

6.7. Personal data processing shall stop when the objective of that processing is achieved or upon the expiry of a period provided for by law, a contract, or the consent of the Personal Data Subject to the processing of their personal data. Should the Personal Data Subject revoke his/her consent to his/her personal data processing, the Bank shall have the right to continue the personal data processing without the Personal Data Subject's consent if such processing is contemplated by an agreement to which the Personal Data Subject is party, beneficiary, or surety, other agreement made between the Bank and the Personal Data Subject, or if the Bank has the right to personal data processing without obtaining the Personal Data Subject's consent pursuant to the grounds provided for 4/, /5/ or other Federal Law.

6.8. Personal data shall be processed in compliance with the requirements of confidentiality, which is understood to mean the obligation not to disclose to any third parties or to disseminate personal data without the consent of the Personal Data Subject, unless otherwise provided by the Russian law.

6.9. The Bank shall ensure the confidentiality of the personal data of the Personal Data Subject on its part, on the part of its affiliates, and on the part of its Employees with access to the personal data of individuals and shall also ensure that the above parties use personal data

exclusively for objectives consistent with the law, a contract, or other agreement entered into with the Personal Data Subject.

6.10. The Bank shall ensure the security of the personal data being processed as part of an integrated, comprehensive system of administrative, technical, and legal measures for the protection of information constituting bank and trade secrets with due regard to the requirements of Personal Data Legislation and the statutory legal acts enacted thereunder. The information security system of the Bank shall be continuously developed and improved based on the requirements of international and national standards of information security and best international practices.

7. Final Provisions

7.1. The Bank, its officials, and its Employees bear civil law and administrative liability and other liability for noncompliance with the principles and terms for the processing of individuals' personal data and for the disclosure or illegal use of personal data pursuant to the Russian law.

7.2. The Policy is publicly available and shall be published on the official website of the Bank, or the present document will be made otherwise accessible without any restrictions.

APPENDIX 1.

Terms and Definitions

Administrative and maintenance activity means internal Bank processes aimed at supporting the current activity of the Bank with goods and material assets (procurement of stationery, office equipment, expendables, household goods, communication services, etc.); organizing document flow (maintaining an archive, libraries, and databases); organizing the maintenance of buildings, premises, and territories (the upkeep, cleaning, decoration, and repair of premises); and organizing the working process.

Bank (operator of the personal data processing) means Sberbank that conducts the personal data processing and defines the objectives of the personal data processing, structure of personal data to be processed, and actions conducted with the personal data.

Close relatives mean relatives in the direct ascending or descending line of kinship (parents and children, grandparents and grandchildren), siblings and half-siblings (brothers ans sisters having the same mother or father)

Candidate means an individual applying for a vacancy at the Bank, whose personal data has been accepted by the Bank.

Client is the term used to refer collectively to a Corporate Client and a Retail Client.

Corporate Client means a legal person, individual entrepreneur, or an individual engaging in private practice in a manner established by the Russian law who has entered into or intends to enter into a contract for the provision of services with the Bank.

Personal data processing means any action (operation) of the Bank or set of actions (operations) done with the personal data with or without the use of automation, including the collection, recording, systematization, accumulation, storage, editing (updating, modification), retrieval, use, communication (Provision, Access), Depersonalization, Blocking, Deletion, and Destruction of personal data. Federal Law No. 152-ФЗ (152-FZ) dated 27 July 2006 'On Personal Data' sets forth the following definitions:

- The blocking of personal data means the temporary cessation of personal data processing (except for instances where processing is necessary for the editing of personal data).
- The depersonalization of personal data means actions that make it impossible to attribute personal data to a specific Personal Data Subject without using additional information.
- The provision of personal data means actions aimed at disclosing personal data to a certain person or a certain group of people.
- The destruction of personal data means actions that make it impossible to recover the contents of personal data in the personal data information system and/or as a result of which the physical media containing personal data are destroyed.

Corporate Client Representative means an individual whose personal data is transferred to the Bank and

- who is a member of the Corporate Client's management bodies

- is an owner/founder/shareholder/member of the Corporate Client
- acts on behalf of the Corporate Client on the basis of a power of attorney/is specified in the sample signature and seal impression card of the Corporate Client.

Bank Employee means an individual who has entered into an employment contract with the Bank.
Personal Data Distribution – actions aimed at disclosing personal data to an undefined group of people.
Retail Client means an individual who has entered into a service contract with the Bank, including the receipt of services by acceding to the terms of a public contract and whose personal data is communicated to the Bank.
Personal Data Subject means an individual who is directly or indirectly identified by the personal data.

APPENDIX 2.

ABBREVIATIONS

CCU means a centrally controlled unit of Sberbank.
CHO means the Central Head Office of Sberbank.
EDIRD means the Bank's electronic database of internal regulatory documents.

ANNEX 3.

REFERENCE DOCUMENTS

1. Constitution of the Russian Federation
2. Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (European Treaty Series No. 108 signed in Strasbourg on 28 January 1981)
3. No. 197-ФЗ (197-FZ) as amended of the Labor Code of the Russian Federation dated 30 December 2001
4. Federal Law No. 152-ФЗ (152-FZ) dated 27 July 2006 'On Personal Data' as amended
5. Regulation No. 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (approved in Brussels on 27 April 2016).