HSBC

APPROVED BY

Acting Chief Executive Officer

HSBC Bank (RR) LLC

_____ E. Rogova

30 December 2015

Personal Data Handling Policy of HSBC Bank (RR) LLC and Implemented Measures to Protect Personal Data

Moscow
2015

1 General Provisions

1.1. “Personal Data Handling Policy of HSBC Bank (RR) LLC and Implemented Measures to Protect Personal Data” (the Policy) determines the general principles and process of personal data handling, and measures to protect personal data implemented by HSBC Bank (RR) (the Bank).

The purpose of this Policy is to protect human and civil rights and freedoms in the process of handling personal data, e.g. to protect human right to personal and family privacy, and to ensure strict and unswerving compliance with Russian laws on personal data.

1.2. This Policy has been developed in accordance with Federal Law dated 27.07.2006 No. 152-FZ “On Personal Data” and other laws and regulations which determine the process of personal data handling and requirements to security of personal data.

1.3. The following terms and definitions are used in this Policy:

Automated processing of personal data	Processing of personal data by means of computer equipment
Personal details database	Any ordered array of personal data, regardless of data carrier and employed means of processing (e.g. archives, card index, electronic databases).
Biometric personal data	Information which reflects a person’s physiological and biological characteristics and can be used to identify such person and which is used by personal data operator to identify a personal data subject.
Blocking of personal data	Temporary suspension of processing of personal data (except if processing is required for adjustment of personal data)
HSBC Group	HSBC Holdings plc, a company established and operating under the laws of England and Wales, and/or HSBC Bank plc, a bank established and operating under the laws of England and Wales, and each entity within the group controlled by that bank.
Access to personal data	Access of certain persons (including employees) to personal data handled by the Bank, on condition of confidential treatment of such personal data.
Personal data system	All personal data contained in databases, and IT technologies and devices used for processing of such personal data
Confidentiality of personal data	Requirement, mandatory for the Bank and any other person / entity which has obtained access to personal data, not to disclose personal data without consent of the personal data subject, unless otherwise required by Russian law.
Data carrier	A physical object used for recording and storage of information containing personal data, including transformed personal data
Depersonalization of personal data	Actions which prevent personal data from being recognized, without additional information, as belonging to any particular personal data subject.
Handling / processing of personal data	Any action / operation or a number of actions / operations performed in respect of personal data with or without automatic devices, including collection, recording, systemization, accumulation, storage, adjustment / amendment / updating, retrieval, use, transfer / distribution / provision, access, depersonalization, blocking, deletion, destruction of personal data.

Publicly available personal data	Personal data which is made publicly accessible by personal data subject or at request of personal data subject, and personal data which must be published or disclosed according to Russian law.
Operator	Government authority, municipal authority, legal entity or physical individual which, on its own or jointly with other parties, organizes processing and/or processes personal data, and which determines the purposes of personal data processing, the type of personal data to be processed, and actions / operations performed in respect of personal data.
Personal data	Any information which directly or indirectly relates to the relevant physical individual (personal data subject)
Distribution / dissemination of personal data	Disclosure of personal data to general public
Personal data subject	Physical individual to whom personal data relates
Cross-border transfer of personal data	Transfer of personal data to a foreign government authority, foreign physical individual or a foreign legal entity located in a foreign country
Destruction of personal data	Actions preventing deleted personal data from being restored in a personal data system, and/or actions resulting in destruction of personal data carriers

2 Status of the Bank and categories of personal data subjects whose personal data is handled by the Bank

2.1 Personal data subjects

2.1.1. The Bank is an operator of personal data owned by the following physical individuals:

- employees of the Bank with whom the Bank has or used to have employment contracts, and persons who provide services in the interests of the Bank under civil law contracts, including such employees and persons whose employment contracts / civil law contracts have been terminated (hereafter referred to as **Employees**);
- close relatives of the Bank's employees whose personal data may be handled in accordance with Russian law (hereafter referred to as the law) and is handled by the Bank as employer according to requirements of state statistic authorities (**Employees' Relatives**);
- candidates for vacant positions at the Bank who have provided, in person or through recruitment agencies (including headhunting web sites), their CVs or profiles (**Candidates**);
- former clients (physical individuals) including bank account owners, depositors, borrowers, clients in securities market transactions, loan security providers and loan guarantors, one-time clients (in transactions not requiring a bank account e.g. currency exchange, money transfers, payments), payees and payers (**Former Clients**);
- beneficial owners, representatives, employees, owners and shareholders of the Bank's corporate clients (legal entities) (**Related Parties**);
- suppliers who are physical individuals, and representatives of suppliers of goods and services for the Bank which are not the Bank's corporate clients, which have a contractual relationship with the Bank, with which the Bank intends to have a contractual relationship

or which intend to have a contractual relationship with the Bank (**Suppliers and their representatives**);

- representatives of any of the abovementioned physical individuals who contact the Bank by order and on behalf of personal data subjects (**Representatives of personal data subjects**);
- visitors of guarded premises of the Bank who do not have permanent access to such premises (**Visitors**).

2.1.2. The Bank is an entity which organizes handling of personal data by order of other operators, including but not limited to:

- government authorities and state extrabudgetary funds to which the Bank transfers Employees' funds or funds to be credited to Employees' accounts (tax offices of the Russian Federal Tax Service, local offices of the Russian Pension Fund, Federal Compulsory Health Insurance Fund, Russian Social Insurance Fund etc.);
- Bank of Russia, Deposit Insurance Agency, RosFinMonitoring, tax offices of the Russian Federal Tax Service, local offices of the Russian Pension Fund and other authorities to which the Bank discloses information, including personal data and bank secrets, in events named in section 26 of the Federal Law dated 02.12.1990 No. 395-1 "On banks and banking";
- military enlistment offices and trade unions to which the Bank discloses personal data in events stipulated by the law.

Personal data is disclosed to abovementioned operators to the extent required by the law, by relevant government authorities and state extrabudgetary funds, within their respective competence. No special consent is required from personal data subjects.

2.1.3. The Bank is not an operator of personal data which is disclosed by its clients or suppliers or their representatives independently upon their own initiative in IT systems of other banks / entities of HSBC Group, including IT systems of parent HSBC Bank.

2.1.4. The Bank shall not be held liable for reliability of personal data which is included in its databases by its counter-parties including other banks / entities of HSBC Group, or by companies which provide information services to the Bank, or for appropriateness of inclusion of such personal data in databases, or for their provision by counter-parties to the Bank under agreement or in accordance with corporate rules of HSBC Group.

2.1.5. The Bank shall not be held liable for appropriateness of publishing, using or for reliability of personal data which has been obtained by the Bank from public sources including generally accessible web sites.

2.2 Principles and purposes of personal data processing

The Bank processes personal data in accordance with the following principles:

2.2.1. Lawful and fair basis for processing of personal data. The Bank takes all necessary measures to comply with the law; it does not process personal data unless permitted to do so by the law, and does not use personal data to harm personal data subjects.

2.2.2. Personal data is processed for specific and legitimate purposes, determined in advance. The Bank processes personal data for the following purposes:

- (for Employees' personal data) - compliance with laws and other regulations including legal requirements to archive storage; performance of the Bank's legally stipulated obligations to government authorities and regulators, clients and suppliers; observance of regulatory requirements to disclosure of information and data including personal data; helping employees with job placement, education, career development, professional training; personal security of employees; control of amount and quality of the work

performed and preservation of property; calculation and payment of salaries and other remuneration; accrual and payment of taxes and insurance fees; compliance with corporate policy regulating HR accounting for overseas banks of HSBC Group and professional training, which makes it possible to observe international standards and requirements of HSBC Group and foreign regulators when employees go on business trips or move to other jurisdictions;

- (for Employees' Relatives) - provision of benefits and guarantees under Russian law to employees who have their own or adopted children, employees with family obligations; voluntary health insurance paid for by the employer; compliance with regulations issued by state statistics authorities;
- (for Candidates) - hiring best suited candidates for vacant positions at the Bank;
- (for Former Clients) - compliance with AML/CTF law; compliance with applicable law e.g. in cross-border transfers of data, and protection of clients' rights and interests;
- (for Related Parties) - performance of agreements with corporate clients; compliance with AML/CTF law; compliance with applicable law e.g. in cross-border transfers of data;
- (for Suppliers and their representatives) - compliance with provisions of the Russian Civil Code which regulate contractual services; performance of agreements with suppliers of goods and services; compliance with applicable law e.g. in cross-border transfers of data;
- (for Representatives of personal data subjects) - Fulfillment of instructions given by representatives of personal data subjects; compliance with applicable law e.g. in cross-border transfers of data (if such transfers are permitted by corporate regulations of HSBC Group);
- (for Visitors) - provision of access to premises of the Bank and St Petersburg Branch for people without a permanent pass; archiving of personal data; compliance with applicable law e.g. in cross-border transfers of data (if such transfers are permitted by corporate regulations of HSBC Group).

2.2.3. The Bank will process only that personal data which agrees with earlier stated processing purposes. The content and volume of processed personal data must agree with stated processing purposes. The Bank will not process personal data for other than stated purposes, and will not process excessive personal data which is not required for stated purposes. The Bank does not collect or process personal data which is not required for purposes listed in section above 2.2.2 of this Policy, and does not use personal data for any other purposes than listed above.

2.2.4. The Bank will not merge databases which contain personal data intended for different incompatible processing purposes.

2.2.5. The Bank makes sure that personal data is accurate, sufficient and relevant for the purposes of processing. The Bank takes all reasonable measures to keep all handled personal data up to date, e.g. permits personal data subjects to exercise their right to access their personal data and to demand adjustment, blocking or destruction of their personal data by the Bank if such personal data is incomplete, out-of-date, inaccurate, unlawfully obtained or not required for processing purposes stated above.

2.2.6. The Bank stores personal data in the form which makes it possible to identify a personal data subject for only as long as required for the purposes of processing, unless a different period of storage is stipulated by the law or an agreement to which the relevant data subject is a party.

2.2.7. The Bank destroys or depersonalizes personal data after achievement of stated purposes or if there is no further need to achieve such purposes, or if the Bank is unable to remove any breaches of legally stipulated data processing procedure, or if a personal data subject withdraws consent to processing of their personal data, unless otherwise stipulated by the law or agreements with personal data subjects.

2.2.8. Personal data handled by the Bank may constitute a bank secret or other type of secret protected by the law. In that case such data is subject to relevant requirements and restrictions according to the law.

2.3 Conditions of personal data processing

2.3.1. The Bank will only process personal data in the following events:

2.3.1.1. If the personal data subject has consented to processing of his/her personal data. The process whereby the Bank obtains consent of a personal data subject is outlined in section 3.2 of this Policy.

2.3.1.2. If the Bank needs to process personal data to be able to exercise / perform its legally stipulated functions, powers and obligations. Such situations include, without limitation, the need to process special types of Employees' personal data to comply with employment law and pension law, to process personal data of Former Clients and to identify Related Parties in accordance with Federal Law dated 07.08.2001 No.115-FZ "On counteraction against money laundering and financing of terrorism".

2.3.1.3. For the purpose of implementing an agreement to which a personal data subject is a party, for the purpose of signing an agreement on the initiative of a personal data subject. Such agreements may include, without limitation, employment contracts and civil contracts with Employees of the Bank.

Pre-contractual work includes recruitment process, in which a personal data subject confirms his/her consent to processing of personal data by completing the Candidate's profile in own hand, or by providing the CV / profile to the Bank or to a recruitment agency, or by publishing it on headhunting web sites, or by sending it to the Bank by e-mail.

2.3.1.4. If the Bank needs to process personal data to exercise any rights and lawful interests of the Bank or third parties or to achieve socially important targets, without prejudice to rights and freedoms of personal data subjects.

2.3.1.5. If personal data is processed for statistical purposes or other research purposes, in which case it must be depersonalized.

2.3.1.6. If access to personal data has been provided to the general public by the personal data subject or at request of personal data subject.

2.3.1.7. If personal data must be published or disclosed according to the law.

2.3.2. The Bank does not disclose personal data to third parties and does not disseminate personal data without consent of personal data subject, unless otherwise required by the law or agreement with personal data subject.

2.3.3. The Bank does not process personal data included in special categories, or personal data which concerns race or nationality, political views, religious or philosophical beliefs, health condition (except if such information determines the Employee's ability to perform his/her job functions or is required for the purposes named in pension law), personal life, Employees' membership in public associations or their labour union activities, except in events clearly stated in the law.

2.3.4. The Bank may process details of personal criminal records only as and when required by the law.

2.3.5. The Bank does not handle biometric personal data.

2.3.6. All personal data collected for cross-border transfers is recorded in databases (e.g. as Excel and Word files or scanned documents) located in the Bank's offices in the Russian Federation, in which the Bank, if necessary, may adjust or update such personal data before cross-border transfer.

2.3.7. No decisions of the Bank which have legal consequences for personal data subjects or otherwise affect the rights and lawful interests of personal data subjects are made by the Bank solely on the basis of automatic processing. Before use, any data which have legal consequences for personal data subjects or otherwise affect the rights and lawful interests of personal data subjects must be checked by authorized employees of the Bank.

3. Processing of Personal Data

Processing of personal data by the Bank is mixed: the Bank may process personal data without automatic devices by recording personal data on separate data carriers, in special sections or on margins on typical forms, or it may process personal data using automatic devices.

3.1. Confidentiality of personal data

3.1.1. Employees of the Bank who have obtained access to personal data must maintain confidentiality of such data.

3.1.2. Confidential treatment is not required for:

- depersonalized personal data;
- publicly accessible personal data.

3.1.3. The Bank may, with consent of personal data subject, request another party to process their personal data, unless otherwise stipulated by the law, under an agreement with such other party according to which such other party must process personal data at the Bank's request in compliance with legally stipulated principles and rules of personal data processing. Amount of personal data transferred to another party for processing, and processing methods used by such other party, should be at a minimum necessary for performance by such party of its obligations to the Bank. Such request of the Bank must include a list of actions / operations which are going to be performed in respect of personal data by such other party, together with processing purposes; the request must also stipulate such party's obligation to maintain confidentiality and security of handled personal data, and requirements to protection of handled personal data in accordance with section 19 of Federal Law dated 27.07.2006 No. 152-FZ "On personal data".

3.1.4. If the Bank requests another party to process personal data the Bank shall be responsible to personal data subject for actions of such other party. The party processing personal data at request of the Bank shall be responsible to the Bank.

3.2. Consent of personal data subject to processing of personal data

3.2.1. A personal data subject decides to provide his/her personal data to the Bank and gives his/her consent to processing of personal data of his/her own free will and in his/her own interests. Consent to processing of personal data must be precise, informed and conscious, and may be given by a data subject in any form permitting to confirm its receipt, unless otherwise required by the law.

3.2.2. If consent to processing of personal data is received from a Representative of personal data subject, the Bank verifies such Representative's powers to give consent on behalf of personal data subject.

3.2.3. If the Bank receives personal data from a client or supplier under an agreement, such client or supplier shall be responsible for appropriateness and reliability of such personal data and for obtaining consent of Related Parties and Representatives of suppliers to transfer of their personal data to the Bank, and such responsibility must be recorded in the agreement between the Bank and such client or supplier.

3.2.4. After receiving personal data from a client or supplier, the Bank is not obliged to inform personal data subjects (or representatives of personal data subjects) which own personal data so

received by the Bank when it begins to process their personal data, because the Bank will rely on such client or supplier to give such information to personal data subjects when obtaining their consent to transfer of their personal data to the Bank. Such obligation of the client and supplier must be recorded in the agreement between the Bank and such client or supplier.

3.2.5. No specifically expressed consent to processing of personal data is required from an Employee because processing is necessary for implementation of agreement to which such Employee is a party, except when an Employee's written consent is required in particular cases of data processing. Such cases requiring Employee's written consent include, without limitation:

- disclosure of an Employee's personal data in public sources e.g. on the official web site of the Bank;
- processing of special categories of personal data, including information about Employee's health condition which is not related to Employee's ability to perform his/her job functions and is not required for purposes named in pension law;
- processing of an Employee's biometric personal data;
- cross-border transfer of personal data to countries which do not provide adequate protection of the rights of personal data subjects, including cross-border transfer to banks / entities of HSBC Group;
- receipt of Employee's personal data from third parties e.g. for the purpose of verification of such personal data or in events when data cannot be obtained directly from the Employee;
- transfer of Employee's personal data to a third party, e.g. for arrangement of business trips, training courses, issue of visas, booking of travel and hotel accommodation, provision of personal data to other banks / entities of HSBC Group etc.;
- disclosure of Employee's personal data to third parties for commercial purposes e.g. to the company which provides HR administration and military registration services in respect of Employees and calculates salary and other income of Employee, to banks which issue and service bank cards for payment of Employee's salary and other income, to insurance companies which provide voluntary health insurance to Employees paid for by the Bank as employer etc.

3.2.6. Employee's written consent to processing of personal data, named in section 3.2.5, may be given as a separate document or provided in the employment contract (or addendum to employment contract), on condition that it must include information required by part 4 section 9 of the Federal Law dated 27.07.2006 No.152-FZ "On personal data".

Employee's written consent to processing of personal data is stored by Human Resources Department in the Employee's personal file.

3.2.7. No specifically expressed consent to processing of personal data has to be obtained from Employees' Relatives if such processing is required by the law (for receipt of alimony, provision of social payments, privileges and benefits etc.) or if such personal data is processed by the Bank as employer in accordance with the requirements of state statistics authorities. In all other events, the Bank must obtain provable (confirmed) consent of Employee's Relatives to processing of their personal data.

3.2.8. No specifically expressed consent to processing of personal data is required from a Candidate because such processing is necessary for signing the employment contract on the initiative of the Candidate as a personal data subject, except when a Candidate's written consent is required in particular cases of data processing. If the Bank decides that the Candidate should be rejected, his/her personal data must be destroyed within 30 days of such decision, unless otherwise required by the agreement with the Candidate or stated in the Candidate's consent to processing of personal data.

3.2.9. No specifically expressed consent to processing of personal data is required from Former Clients because such their personal data must be processed in accordance with AML/CTF law.

3.2.10. Personal data of Related Parties, Suppliers and Suppliers' representatives contained in central state registers of legal entities and individual entrepreneurs is regarded as publicly available and generally accessible, except number of personal ID document, date of issue, issuing authority, together with information contained in public sources including web sites. No confidential treatment or consent of personal data subjects is required for processing of such data.

In all other events, the Bank must obtain consent of Related Parties and Suppliers' representatives as personal data subjects, except those who have signed agreements with the Bank, or have provided powers-of-attorney authorizing them to act on behalf and by order of the Bank's clients or suppliers, or have personally inserted their details in electronic forms on the web site(s) of banks / entities of HSBC Group, and have thereby taken implicative action confirming their consent to processing of personal data named in the text of the relevant agreement, power-of-attorney or registration form on the web site. A representative's consent to transfer of his/her personal data to the Bank and to processing of such personal data by the Bank may be obtained by the represented client or supplier, in which case the Bank is not required to obtain data subject's consent to processing of his/her personal data.

3.2.11. Representatives of personal data subjects express their consent to processing of their personal data in the form of implicative actions i.e. provision of a power-of-attorney or on the basis of powers given to them by agreement or other legally binding document to act on behalf and by order of personal data subjects, and personal ID document.

3.2.12. Visitors express their consent to processing of their personal data in the form of implicative actions i.e. presentation of their personal ID document and provision of information requested from them during visit to the Bank's premises.

3.2.13. The Bank does not have to obtain consent of personal data subjects to processing of their personal data if such personal data is reasonably requested from the Bank, in accordance with their powers, by the Bank of Russia, tax authorities, prosecution authorities, law enforcement authorities, investigation authorities, security forces, by state labour inspectors in their work to supervise and control compliance with labour law, or by other bodies authorized to request information in accordance with their legally stipulated competencies.

3.2.14. If requests for personal data are received from organizations which do not have the relevant powers, the Bank must obtain consent of personal data subject (who is not an Employee of the Bank), in any provable form, to processing of his/her personal data, and must notify recipients of personal data that they may use such data only for claimed purposes; the Bank also may demand proof from such recipients that this rule is / will be observed. The process whereby the Bank obtains consent of its Employees to transfer of their personal data to other parties is outlined in section 3.2.5 of this Policy.

3.2.15. A personal data subject may withdraw his/her consent to processing of personal data if such processing is not required by the law or by agreement with the Bank to which such data subject is a party. The Bank may continue processing of personal data after withdrawal of the data subject's consent in events listed in sections 2-11 part 1 article 6, part 2 article 10 and part 2 article 11 of the Federal Law dated 27.07.2006 No.152-FZ "On personal data".

3.2.16. In all events, the Bank is obliged to present proof of obtained consent of a personal data subject to processing of his/her personal data, or present proof of facts listed in Federal Law dated 27.07.2006 No.152-FZ "On personal data".

4. Rights of Personal Data Subjects

5.1. A personal data subject has the right to receive information which concerns processing of his/her personal data. A personal data subject has the right to demand that his/her personal data

should be adjusted, blocked or destroyed by the Bank if such personal data is incomplete, out-of-date, inaccurate or not required for claimed purposes, and may take legally permitted measures to defend his/her rights.

5.2. If a personal data subject believes that the Bank handles his/her personal data with violation of the law or otherwise violates his/her rights or freedoms, such personal data subject may report such inappropriate actions or omissions of the Bank to the regulatory authority in charge of protection of the rights of personal data subjects, or may file legal claims.

5.3. A personal data subject has the right to protection of his/her rights and lawful interests, including the right to compensation of losses and/or emotional damages through legal proceedings.

5. Implemented Measures to Protect Personal Data

5.1. Security of personal data handled by the Bank is achieved by means of legal, organizational and technical measures which are necessary and sufficient to ensure compliance with laws on protection of personal data.

5.2. Such legal measures include:

- development of the Bank's corporate regulations to comply with applicable law, including Personal Data Handling Policy;
- avoidance of any methods of processing of personal data which contradict the purposes stated in the Policy.

5.3. Such organizational measures include:

- appointment of the officer in charge of personal data handling;
- appointment of the officer responsible for security of personal data in personal data systems;
- restricting the number of Bank employees who have access to personal data, and organization of authorization-based access system;
- informing Bank employees directly involved in handling of personal data about requirements of personal data laws, including requirements to protection of personal data, this Policy, other corporate regulations of the Bank on handling of personal data;
- training for all group of employees directly involved in handling of personal data on the rules of personal data handling and on security of handled personal data;
- inclusion of obligations to maintain security of personal data, and of liability for breaches of existing procedures, in job descriptions of Bank employees;
- formal regulation of personal data handling processes;
- organization of registration and storage of personal data carriers to prevent theft, replacement, unauthorized copying or destruction;
- identification of the types of threats to personal data which are relevant to personal data systems, with consideration of potential damage to personal data subjects which may be inflicted as a result of breached security requirements; assessment of the level of security of personal data;
- identification of the types of threats to personal data processed within personal data systems, creation of individual threat models on their basis;
- locating technical means of personal data processing on guarded premises;
- restricting access of strangers to premises of the Bank; preventing any access of strangers to premises where personal data is handled and where technical means of processing are located – without control by Bank employees.

5.4. Technical measures include:

- actual implementation of the requirements to protection of personal data processed within personal data systems – to achieve planned security levels, development of individual model of relevant threats, and introduction of a personal data protection system for security levels stipulated by the Russian government in respect of personal data handled within personal data systems;
- use of successfully assessed information security tools to neutralize relevant threats;
- assessment of the efficiency of implemented measures for security of personal data before introduction of personal data systems;
- implementation of authorization-based access of employees to personal data processed within IT systems, to hardware and software tools for data protection;
- registration and recording of actions performed in respect of personal data by users of IT systems in which personal data is processed;
- detection of malware (use of anti-virus software) in all parts of the Bank's IT system which have the required technical capability;
- secure inter-network screens (use of firewalls);
- detection of intrusions into the Bank's IT system which violate or create the conditions for violation of existing requirements to security of personal data;
- encryption of personal data transmitted via unsecured telecom channels e.g. the Internet, including both personal data which is received from clients and suppliers for purposes of contractual performance and personal data which is sent to clients and suppliers;
- recovery of personal data which has been modified or destroyed as a result of unauthorized access (system of backup and recovery of personal data);
- control of compliance with these requirements (independently or with contract-based involvement of organizations licensed to provide technical protection for confidential information), at least once every 3 years.

6. Final Provisions

6.1. Other obligations and rights of the Bank as operator of personal data and entity which organizes handling of personal data by order of other operators are determined by Russian laws on personal data.

6.2. Employees of the Bank who breach any laws on personal data of this Policy shall bear civil, criminal, administrative, disciplinary or other responsibility as may be contemplated by the law.

6.3. Legal entities which violate their contractual obligation to maintain confidentiality of personal data shall bear civil responsibility in accordance with Russian law.

6.4. This Policy shall be updated[1] in the following events:

- after changes in the laws on handling and protection of personal data;
- after receipt of orders to remove any deficiencies related to scope of this Policy;
- by resolution of managers of the Bank;
- after changes to organizational structure of the Bank which affect departments involved in implementation of this Policy;
- after changes to / introduction of structure of IT systems and/or telecommunication systems, after implementation of new personal data processing technologies;
- after emergence of a need to adjust the process of personal data handling, in connection with business activity of the Bank;

[1] Updating means alignment of this Policy with Russian laws, industry standards, regulations of the Bank, business requirements etc.

- after occurrence of incidents, discovery of vulnerabilities, after other material information security events, by resolution of managers of the Bank.

Any changes to this document shall be made and approved according to the procedure established by the Bank.