РОСБАНК

С0−Общедоступная информация

C0–Public Information

УТВЕРЖДЕНА
приказом Председателя Правления
от 26 июля 2016 г. №572

APPROVED
By order of the Chairman of the
Management Board
No.572 dd. July 26th, 2016

ОДОБРЕНА
решением Комитета по развитию
продуктов и технологий
ПАО РОСБАНК
протокол от 06 июля 2016 г. №19-1

VALIDATED
By resolution of Product and Technologies
Development Committee of
PJSC ROSBANK
Minutes No. 19-1 dd. June 06th, 2016

ПОЛИТИКА ПАО РОСБАНК
в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных

POLICY of PJSC ROSBANK
on processing of personal data and requirements to personal data protection

№ POL-RB-1728

Версия (version) 2.0

Информационный лист

Область действия	Головной офис, подразделения сети
Сфера действия	Поддержка и обеспечение
Направления деятельности	Безопасность
Уровень иерархии	Первый
Краткое содержание документа	Документ определяет политику ПАО РОСБАНК в отношении обработки персональных данных и содержит общие сведения о реализуемых требованиях к защите персональных данных
Подразделение - владелец	Департамент информационной безопасности
Подразделение - исполнитель	Департамент информационной безопасности
Дата введения в действие документа	По истечении 5 рабочих дней с даты издания приказа
Дата окончания действия документа	Не определена
Отмененные документы	ПОЛ-РБ-33 Политика обработки и обеспечения безопасности персональных данных в ОАО АКБ «РОСБАНК», Утверждена Председателем Правления ОАО АКБ «РОСБАНК» 28 июня 2012 г. Версия 1.0
Используемые типовые формы	Отсутствуют

Information list

Scope of application	Head Office, network outlets
Sphere of application	Support and maintenance
Focus of application	Security
Level of hierarchy	First
Summary of the Document	The Document determines the policy of PJSC ROSBANK on processing of personal data and carries an overview of requirements to personal data protection
Owner	Information Security Department
Unit in charge of execution	Information Security Department
Date of validity	Upon expiration of 5 business days following issuance of the Order
Expiration date	Not determined
Superseded documents	POL-RB-33 Policy on processing of personal data and provision of security of personal data in OJSC JSCB ROSBANK approved by the Chairman of the Management Board of OJSC JSCB ROSBANK on June 28, 2012. Version 1.0
Applicable standard forms	None

СОДЕРЖАНИЕ

CONTENTS

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение и область действия

1.1.1. Настоящая Политика определяет общие принципы обработки персональных данных и содержит сведения о реализуемых требованиях к защите персональных данных в ПАО РОСБАНК. Целью принятия Политики является обеспечение прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.1.2. Действие Политики распространяется на Головной офис и подразделения сети ПАО РОСБАНК. Действие Политики распространяется на все персональные данные субъектов, обрабатываемые в Банке с применением средств автоматизации и без применения таких средств.

1.1.3. Политика обработки и обеспечения безопасности персональных данных в Банке (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», другими законодательными и нормативными правовыми актами (далее – законодательство), определяющими порядок работы с персональными данными и требования к обеспечению их безопасности.

1.1.4. Политика подлежит пересмотру и актуализации с периодичностью не реже 1 (одного) раза в 3 (три) года или при изменении законодательства. Поддержание в актуальном состоянии Политики обеспечивает Департамент информационной безопасности.

1.1.5. К настоящей Политике предоставляется неограниченный доступ любому лицу, желающему с ней ознакомиться.

1.1.6. Настоящая Политика размещается на официальном сайте Банка в сети Интернет, а также в доступном для посетителей месте в каждом из офисов Банка, в которых производится обслуживание клиентов.

1. GENERAL PROVISIONS

1.1. Purpose and scope of application

1.1.1. This Policy defines the general principles of processing of personal data and carries an overview of the requirements to personal data protection in PJSC ROSBANK. The objective of the Policy is to secure human and civil rights and freedoms upon processing personal data, including protection of right to privacy and personal and family secrets.

1.1.2. The scope of application of this Policy covers the Head Office and network units of PJSC ROSBANK. This Policy shall apply to all personal data of subjects processed at the Bank with or without use of automated facilities and equipment.

1.1.3. The Policy on processing of personal data and personal data protection in the Bank (hereinafter referred to as the Policy) was developed in accordance with Federal law No. 152-FZ of July 27, 2006 *On Personal Data* and other legislative and regulatory legal acts (hereinafter referred to as the Legislation), which determine the procedure for processing of personal data and define the requirements to personal data protection.

1.1.4. This Policy shall be subject to reviewing and updating not less than once per every three years, or following changes in the Legislation. The Information Security Department shall be in charge of updating of this Policy.

1.1.5. Access to this Policy shall be granted to any person who wishes to familiarize himself/herself with it.

1.1.6. This Policy shall be placed on the official site of the Bank in Internet, as well as in places open for public access in every office of the Bank which provides services to its clients.

1.2. Термины и определения

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

база персональных данных – упорядоченный массив персональных данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных);

Банк – ПАО РОСБАНК, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

конфиденциальность персональных данных – обязательное для соблюдения Банком или иным, получившим доступ к персональным данным лицом, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством;

обезличивание персональных данных – действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных;

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление,

1.2. Terms and Definitions

Automated processing of personal data means handling of personal data with use of means of computer technologies and equipment;

Personal details database means an ordered array of personal data independent of any type of physical data storage media and means of data processing (archives, card indices, electronic databases);

Bank stands for PJSC ROSBANK, which organizes and/or performs, independently or in conjunction with other entities, processing of personal data, as well as defines the objectives of processing of personal data, composition of personal data subject to processing, actions (operations) with personal data;

Blocking personal data means temporary suspension of processing of personal data (except for cases where data processing is necessary for rectification of such data);

Information system of personal data constitutes an aggregate of personal data storage in databases and a set of information technologies and technical tools for their processing;

Confidentiality of personal data means an obligatory requirement to the Bank or any person with an authorized access to personal data, not to disclose to third persons and not to disseminated personal data without a consent of the subject of personal data, unless otherwise specified by the Legislation;

Depersonalization (anonymization) of personal data means actions as a result of which it is impossible to determine ownership of personal data of a specific subject of such data without use of additional information;

Processing of personal data means any action (operation) or a set of actions (operations) performed with or without use of means of automation, including collection, recording, filing, accumulation, storage, rectification (updating, modification), retrieval, utilization, transmission (dissemination, provision, access), depersonalization, blocking, deletion, destruction of personal data;

хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

предоставление персональных данных – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц;

субъект персональных данных – физическое лицо, к которому относятся персональные данные;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;

уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) результате которых уничтожаются материальные носители персональных данных.

Personal data constitutes any information which directly or indirectly relates to a specific person or an identified individual (personal data subject/owner);

Provision of personal data includes actions aimed at disclosure of personal data to a specific person or a scope of persons;

Dissemination of personal data comprises actions aimed at disclosure of personal data to an indefinite scope of persons;

Subject (owner) of personal data means an individual to which personal data is related;

Cross-border transfer of personal data means transmission of personal data to an authority in the territory of a foreign state, to a foreign individual or legal entity;

Destruction of personal data means actions as a result of which it is impossible to of personal data in the information system of personal data and/or as a result of which physical personal data media are destroyed.

2. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных в Банке осуществляется на основе принципов:

- законности и справедливой основы;
- ограничения обработки персональных данных достижением конкретных, заранее определённых и законных целей;
- недопущения обработки персональных данных, несовместимой

2. PRINCIPLES AND CONDITIONS OF PERSONAL DATA PROCESSING

2.1. Processing of personal data I performed in the Bank on the basis of the following principles:

- Legality and fairness;
- Compliance with predetermined and legitimate purposes;
- Strict compliance with the objectives of personal data collection;

с целями сбора персональных данных;

— недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

— соответствия содержания и объёма обрабатываемых персональных данных заявленным целям обработки;

— недопущения обработки избыточных персональных данных по отношению к заявленным целям их обработки;

— обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;

— хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

— уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Банком допущенных нарушений персональных данных, в случае отзыва субъектом своего согласия на обработку персональных данных, если иное не предусмотрено законодательством или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

2.2. Все персональные данные при их сборе записываются в базы данных, находящиеся на территории Российской Федерации, в которых происходит также при необходимости их уточнение, изменение или обновление, а также извлечение для последующей трансграничной передачи персональных

— Inadmissibility of integration of databases which contain incompatible personal data;

— Consistency of the content and volume of processed personal data with the stated objectives of processing;

— Inadmissibility of processing of excessive personal data with regard to the stated objectives of processing;

— Assurance of accuracy, sufficiency and relevance of personal data to the objectives of their processing;

— Storaging of personal data in the form which allows to identify the subject of personal data for the period which does not exceed the objectives of personal data processing, if the duration of retaining of personal data is not specified by the Legislation, contract, to which the subject of personal data is a party, beneficiary or guarantor;

— Destruction or depersonalization of personal data upon achieving the goals of their processing in case it is impossible for the Bank to remedy violation of personal data in the context of the subject's of personal data revocation of his/her consent to process personal data, unless otherwise specified by the Legislation or contract, to which the subject of personal data is a party, beneficiary or guarantor.

2.2. Upon their collection, all personal data shall be recorded in the databases located in the territory of the Russian Federation, with such data rectified, modified or updated for the purpose of subsequent cross-border transfer of such personal data.

данных.

2.3. Обработка персональных данных в Банке допускается в следующих случаях:

— обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

— обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством на Банк функций, полномочий и обязанностей;

— обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством об исполнительном производстве;

— обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации Банком своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

— обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

— обработка персональных данных необходима для осуществления прав и законных интересов Банка или третьих лиц либо для достижения общественно значимых целей при условии, что при

2.3. It shall be allowed to process personal data in the Bank in the following cases:

— Processing of personal data is conducted with the consent of the owner of subject of personal data to their processing;

— Personal data processing is required for the purposes established by an international treaty of the Russian Federation or law, in pursuit and discharge of the statutory functions of the Bank, its mandates and obligations;

— Personal data processing is necessary for the purposes of delivery of justice, execution of court orders and acts of other bodies or officials, subject to execution in accordance with the statutory court enforcement proceedings;

— Personal data processing is necessary for performance of a contract a party to which or a beneficiary is represented by a subject of personal data, including for exercise by the Bank of its right to cession of rights (receivables) under such contract, as well as for concluding a contract at the initiative of the owner of personal data or a contract under which such owner of personal data shall act as a beneficiary or a guarantor;

— Personal data processing is necessary to protect life, health or vital interests of a subject of personal data, in case it is not possible to obtain the consent of such subject of personal data;

— Personal data processing is necessary to exercise rights and legitimate interests of the Bank or third persons or to achieve objectives of public importance, provided the rights and freedoms of the subject of personal data shall not be violated;

— Processing of personal data is performed with regard to data an access to which is provided by the owner of personal data or pursuant to his/her request to an unlimited range of

этом не нарушаются права и свободы субъекта персональных данных;

— осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе[1];

— осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством.

persons[2];

— Processing of personal data is performed with regard to data subject to publication or mandatory disclosure in accordance with the legislation.

2.4. Банк не раскрывает персональные данные субъекта третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством.

2.4. The Bank shall not disclose personal data of a subject to third persons and shall not disseminate personal data without a consent of the subject of personal data, unless otherwise established by law.

2.5. Банк поручает обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством, на основании заключаемого с этим лицом договора поручения обработки персональных данных. Лицо, осуществляющее обработку персональных данных по поручению Банка, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных».

В случае, если Банк поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Банк. Лицо, осуществляющее обработку персональных данных по поручению Банка, несет ответственность перед Банком.

2.5. The Bank shall, upon the consent of the subject of personal data, entrust the processing of personal data to another person, unless otherwise established by law, on the basis of a contract on processing of personal data concluded with such person. The person who processes personal data on an instruction of the Bank shall comply with the principles and rules of personal data processing established by the Federal Law *On Personal Data*.

In case the Bank entrusts processing of personal data to another person, the Bank shall be liable to the subject of personal data for person's actions. The person in charge of processing of personal data on an instruction of the Bank shall be liable for its actions to the Bank.

2.6. Банком не обрабатываются персональные данные, относящиеся к специальным категориям:

- расовая принадлежность;
- национальная принадлежность;
- политические взгляды;
- религиозные или философские

2.6. The Bank shall not process personal data which relate to special categories:

- race;
- ethnic origin;
- political views;
- religious beliefs and philosophical views;

[1] Здесь и далее – общедоступные персональные данные

[2] Hereinafter means publicly available personal data.

убеждения;

- состояния здоровья (за исключением данных о состоянии здоровья работников Банка в случаях, предусмотренных Трудовым кодексом Российской Федерации);
- интимная жизнь;

а также иные персональные данные о частной жизни, о членстве субъектов персональных данных в общественных объединениях или их профсоюзной деятельности.

Обработка указанных категорий персональных данных допускается в случаях, если:

- она прямо предусмотрена законодательством;
- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными.

2.7. Обработка персональных данных о судимости может осуществляться Банком исключительно в случаях и в порядке, определяемых законодательством.

2.8. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность - биометрические персональные данные - обрабатываются Банком только при наличии согласия субъекта в письменной форме или в случае, когда такая обработка предусмотрена законодательством, в том числе законодательством о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

2.9. Создание фото- и видео- изображений производится Банком с целью контроля соблюдения законности и правопорядка, а также предотвращения противоправных действий, экстремистских проявлений и террористических актов, и последующей передачи в правоохранительные органы в случае необходимости. Указанные фото- и видео- изображения не используются с целью идентификации субъектов персональных данных и не рассматриваются Банком как

- health status (except for data about health of the Bank employees incases specified by the Labor Code of the Russian Federation);
- intimacy;

as well as other personal data about private life, membership in public associations or union activity.

Processing of such categories of personal data shall be allowed in cases, where:

- personal data is specified by law;
- the subject of personal data gave his/her written consent to processing of his/her personal data;
- personal data constitute public data.

2.7. The Bank may process personal data relating to a record of convictions only in cases and according to the procedure determined by the Legislation.

2.8. Data about physiological and biological properties of a human being based on which his/her such persona may be identified (biometric personal data) shall only be processed by the Bank on the basis of a written consent of the subject of personal data or in the case where such processing is established by the Legislation, including by the legislation on the procedure of exit from/entry to the Russian Federation.

2.9. The Bank shall produce photo and video images for the purpose of control of compliance and law-enforcement, as well as prevention of wrongful acts, extremist actions and acts of terrorism and subsequent presentation of such images to law-enforcement bodies in cases of need. The Bank shall not such photo and video images for the purpose of identification of subjects of personal data as biometric personal data.

биометрические персональные данные.

2.10. Банк осуществляет трансграничную передачу персональных данных работников в организацию Societe Generale S.A. (Париж, Франция), созданную по законодательству Франции, являющуюся контролирующим акционером Банка. Франция является стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных ETS-108 и обеспечивает адекватную защиту прав субъектов персональных данных.

Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться Банком в случаях:

- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- исполнения договора, стороной которого является субъект персональных данных, в том числе при осуществлении по поручению клиента банковских операций с иностранными банками.

3. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБЕСПЕЧИВАЕМЫЕ БАНКОМ

3.1. Субъект персональных данных (здесь и далее по тексту под субъектом персональных данных понимается как сам субъект персональных данных, так и его законный представитель: родитель, опекун, попечитель и иные лица, полномочия которых установлены законодательством Российской Федерации) принимает решение о предоставлении его персональных данных и даёт Банку согласие на их обработку Банком свободно, своей волей и в своём интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством.

2.10. The Bank shall perform a trans-border transfer of personal data of its employees to the organization of Societe Generale S.A. (Paris, France) established under the legislation of France, which shall act as a controlling shareholder of the Bank. France shall act as a party to the Convention of the Council of Europe on protection of individuals upon automated processing of personal data *ETS-108* and shall ensure an adequate protection of the rights of owners of personal data.

The Bank may perform a trans-border transfer of personal data to the territory of foreign states which do not provide an adequate protection of the rights of owners of personal data, in the following cases:

- Existence of a written consent on the part of the owner of personal data to a trans-border transfer of his/her personal data;
- Execution of a contract to which the owner of personal data is a party, including upon the client's instruction to perform bank transactions with foreign banks.

3. THE RIGHTS OF THE SUBJECT OF PERSONAL DATA ENSURED BY THE BANK

3.1. A subject of personal data (hereinafter a subject of personal data is understood to mean his/her lawful representative, i.e. a parent, a guardian, a trustee, and other persons whose powers are established by the Legislation of the Russian Federation) shall take a decision to provide his/her personal data and gives his/her consent to the Bank to process his/her personal data on a voluntary basis, at his/her own will and for his/her own benefit. The subject of personal data or his/her representative may give his/her consent to process personal data in any form which allows to confirm the receipt of such consent, unless otherwise specified by the Legislation.

The Bank shall bear an obligation to provide evidence of the receipt of a consent of the subject of personal data to

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований на обработку, предусмотренных законодательством, возлагается на Банк.

3.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, если такое право не ограничено в соответствии с законодательством. Субъект персональных данных вправе требовать от Банка уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством меры по защите своих прав.

3.3. Обработка Банком персональных данных в целях продвижения товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных.

Банк обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в вышеуказанных целях.

3.4. В Банке запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных законодательством, или при наличии согласия в письменной форме субъекта персональных данных.

3.5. Если субъект персональных данных считает, что Банк осуществляет обработку его персональных данных с нарушением требований законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие

process such data or evidence of existence of grounds for processing specified by the Legislation.

3.2. A subject of personal data shall be entitled to obtain information relating to his/her personal data, unless such right is not restricted by the Legislation. A subject of personal data shall be entitled to demand from the Bank to update his/her personal data, block or destroy such data, if such personal data is incomplete, obsolete, inaccurate, obtained in an unlawful way, or if such data is irrelevant for the stated purposes of processing, as well as shall be entitled to resort to remedies of protection of his/her rights.

3.3. The Bank shall be allowed to process personal data for the purpose of promotion of goods, work, services on the market by way of direct contacts with potential users with reliance on means of communication only on the condition of a prior consent of the subject of personal data.

The Bank shall be obliged to immediately discontinue personal data processing following the demand of the subject of such personal data for the above purposes.

3.4. It shall be prohibited to take decisions in the Bank on the basis of exclusively automated processing of personal data which gives rise to legal consequences with regard to the subject of personal data or otherwise affect his/her rights and legitimate interests, with the exception of cases specified by the Legislation, or in case of existence of a written consent on the part of the subject of personal data.

3.5. If the subject of personal data holds the opinion that the Bank processes his/her personal data in violation of the legislative requirements or violates his/her rights and freedoms, such subject of personal data shall be entitled to lodge an appeal against the actions or omission on the part of the

Банка в Уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4. СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Безопасность персональных данных, обрабатываемых Банком, обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты персональных данных, выявлением и предотвращением инцидентов, связанных с неправомерным доступом к персональными данными и неправомерных действий с ними.

4.2. Для целенаправленного создания в Банке неблагоприятных условий и труднопреодолимых препятствий для нарушителей, пытающихся осуществить несанкционированный доступ к персональным данным в целях их получения, модификации, блокирования, уничтожения, заражения вредоносным программным кодом и совершения иных несанкционированных действий, Банком применяются следующие организационно-технические меры:

- назначение должностных лиц, ответственных за организацию обработки и обеспечение безопасности персональных данных;
- ограничение состава работников, обрабатывающих персональные данные и имеющих доступ к персональным данным при выполнении своих трудовых обязанностей, регламентация порядка предоставления такого доступа;
- ознакомление работников с требованиями законодательства и внутренних нормативных документов Банка по обработке и защите персональных данных;

Bank to the Authorized Body for Protection of Rights of Subjects of Personal Data (*Roskomnadzor*), or through the court.

The subject of personal data shall be entitled to protect his/her rights and legitimate interests, including his/her right to indemnity of losses and/or compensation of moral damage through the court.

4. OVERVIEW OF REQUIREMENTS TO PERSONAL DATA PROTECTION

4.1. Security of personal data processed by the Bank shall be ensured on the basis of implementation of legal, administrative and technical measures necessary to meet the requirements of the federal Legislation on protection of personal data, to identify and prevent incidents associated with an unauthorized access to personal data and illegal actions therewith.

4.2. For the purpose of well-directed creation in the Bank of conditions which deny offenders access to personal data with the aim of obtaining, modification, blocking, destruction, infection of such data with malware codes and unlawful actions, the Bank shall take the following administrative and technical measures:

- Appointment of officers responsible for organization of processing and security of personal data;
- Restriction of the range of employees who process personal data and who have access to personal data in the course of execution of their job responsibilities, as well as regulation of the procedure for granting such access;
- Familiarization of employees with legislative requirements and the Bank's internal regulatory documents on processing and protection of personal data;
- Provision of accounting and storaging of physical media for keeping personal data and establishment o a procedure for handling such data designed to prevent their theft, spoofing, unauthorized copying and destruction;

- обеспечение учёта и хранения материальных носителей персональных данных и установление порядка обращения с ними, направленного на предотвращение их хищения, подмены, несанкционированного копирования и уничтожения;
- определение угроз безопасности персональным данным при их обработке, формирование на их основе частных моделей угроз и постоянное поддержание их актуальности;
- разработка на основе модели угроз системы защиты персональных данных для соответствующего уровня защищенности персональных данных;
- регулярная проверка готовности и эффективности используемых средств защиты информации;
- реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- парольная защита доступа пользователей к информационной системе персональных данных;
- регистрация и учёт действий пользователей информационных систем персональных данных;
- применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;
- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;
- осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ и программных закладок;
- применение межсетевого экранирования;

- Identification of threats to security of personal data upon their processing, formation on their basis of particular models of threats and continuous updating thereof;
- Development on the basis of the model of threats a system of personal data protections designed to ensure the requisite level of security of personal data;
- Regular testing of readiness and efficiency of utilized data protection facilities;
- Implementation of a system of authorization of users' access to information resources, hardware and software means of processing and protection of information;
- Password protection of user's access to the information system of personal data;
- Registration and individual accountability of users of information systems of personal data;
- Application of a mechanism of control of access to communication ports, data input/output devices, removable data media and external memory;
- Application, where necessary, facilities of cryptographic protection of information to ensure protection of personal data in the course of their transmission via open channels and storaging on data media и хранении на машинных носителях информации;
- Exercise of anti-virus control, prevention of infiltration into the corporate network of malware and malicious logic;
- Application of firewalling;
- Detection of intrusions into the Bank's corporate network which breach or create prerequisites for violation of established requirements to personal data security;
- Performance of an analysis of the level of protection of the Bank's information systems of personal data with use of specialized software (security

- обнаружение вторжений в корпоративную сеть Банка, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищённости информационных систем персональных данных Банка с применением специализированных программных средств (сканеров безопасности);
- централизованное управление системой защиты персональных данных;
- резервное копирование информации;
- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;
- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей персональных данных;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям по безопасности;
- систематическое проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;
- размещение технических средств обработки персональных данных в пределах охраняемой территории;
- организация пропускного режима на территорию Банка, охраны помещений и собственно технических средств обработки персональных данных;
- поддержание технических средств

scanners);

- Centralized management of the system of personal data protection;
- Data backuping;
- Recovery of personal data which were modified or destroyed as a result of unauthorized access to such data;
- Training of employees who use information security facilities employed in information systems of personal data to apply rules of personal data handling;
- Accounting of utilized data protection facilities, operating and technical documentation on such facilities, personal data media;
- Utilization of data protection facilities tested with use of procedure of compliance with the security requirements;
- Systematic monitoring of users' actions, performance of investigation of instances of violation of requirements to security of personal data;
- Location of technical facilities for processing of personal data within the perimeter of secured premises;
- Arrangement mode of access to the premises of the Bank, security of premises and technical facilities of personal data protection;
- Maintenance of constant-readiness status of technical facilities of security, alarm systems and video-surveillance devices.

охраны, сигнализации помещений в состоянии постоянной готовности, ведение видеонаблюдения.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. Иные права и обязанности Банка, связанные с обработкой им персональных данных, определяются законодательством в области персональных данных.

5.2. Должностные лица Банка, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую и уголовную ответственность в порядке, установленном законодательством и внутренними нормативными документами Банка.

5. CONCLUDING PROVISIONS

4.3. Other rights and responsibilities of the Bank connected with processing of personal data shall be determined by the Legislation on personal data.

4.4. The Bank officials guilty of violation of the norms which regulate personal data protection, shall bear material, disciplinary, administrative, civil and criminal liability in accordance with the procedure established by law and the Bank's internal regulatory documents.