УТВЕРЖДЕНО

Решением Правления

АО БАНК «МОСКВА-СИТИ»

ПРОТОКОЛ № 18-08

от 18 августа 2023 г.

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ АКЦИОНЕРНОГО ОБЩЕСТВА АКЦИОНЕРНЫЙ ИНВЕСТИЦИОННЫЙ БАНК МОСКОВСКОГО МЕЖДУНАРОДНОГО ДЕЛОВОГО ЦЕНТРА «МОСКВА-СИТИ» (АО БАНК «МОСКВА-СИТИ»)

Москва
2023

ОГЛАВЛЕНИЕ

1. Общие положения

1.1. В целях поддержания деловой репутации и гарантирования выполнения норм федерального законодательства в полном объеме АО БАНК «МОСКВА-СИТИ» (далее – Банк или Оператор) считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.2. Обработка и обеспечение безопасности информации, отнесенной к персональным данным, осуществляется в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. № 152 ФЗ «О персональных данных».

1.3. Настоящая политика в области обработки и защиты персональных данных в АО БАНК «МОСКВА-СИТИ» (далее – Политика) характеризуется следующими признаками:

- разработана в целях обеспечения реализации требований законодательства РФ и Банка России в области обработки персональных данных, а именно любой информации, относящейся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);
- раскрывает основные категории персональных данных, обрабатываемых Оператором, цели, способы и принципы обработки Оператором персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке;
- является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке персональных данных.

1.4. Настоящая Политика Банка в области обработки персональных данных разработана в соответствии с требованиями:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федерального закона от 02.12.1990 № 395-1-ФЗ «О банках и банковской деятельности»;
- Федерального закона от 30.12.2004 № 218-ФЗ «О кредитных историях»;

• Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

• Федерального закона от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле»;

• Федерального закона от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг»;

• Федерального закона от 23.12.2003 № 177-ФЗ «О страховании вкладов физических лиц в банках РФ»;

• Федерального закона от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

• Стандарта Банка России СТО БР ИББС 1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»;

• Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

• Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

• Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

• Постановления Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

• Устава Банка.

2. Информация о Банке

Наименование: АКЦИОНЕРНОЕ ОБЩЕСТВО АКЦИОНЕРНЫЙ ИНВЕСТИЦИОННЫЙ БАНК МЕЖДУНАРОДНОГО ДЕЛОВОГО ЦЕНТРА «МОСКВА-СИТИ» (сокращенное наименование: АО БАНК «МОСКВА-СИТИ») ИНН: 7703033450 ОГРН 1027739045124

Фактический адрес: 115114, Москва, 2-й Кожевнический переулок, д. 7

Тел.: +7 (495) 981-85-01

3. Термины и определения

Автоматизированная обработка ПДн – обработка персональных данных с помощью средств вычислительной техники.

Блокирование ПДн – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Биометрические ПДн – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установитьего личность.

Информационная система ПДн – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка ПДн – 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, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – Банк, осуществляющий обработку персональных данных и определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

ПДн, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных путем предоставления согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом.

Предоставление ПДн – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение ПДн – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Трансграничная передача ПДн – передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

4. Категории субъектов персональных данных, персональные данные которых обрабатываются Банком. Цели обработки персональных данных.

4.1. Банком осуществляется обработка полученных в установленном Законом от 27.07.2006 152- ФЗ «О персональных данных» порядке персональных данных, принадлежащих следующим категориям субъектов персональных данных:

- Физические лица, состоящие (состоявшие) с Банком в договорных гражданско-правовых отношениях, трудовых отношениях, кандидаты на замещение вакантных должностей;
- Физические лица - участники Банка, члены органов управления, лица, осуществляющие контроль за деятельностью банка, аффилированные и иные связанные с Банком лица;
- Физические лица, обратившиеся в Банк с целью получения информации от Банка;
- Физические лица, являющиеся Клиентами (потенциальными клиентами) Банка (выгодоприобретатели, бенефициары, поручители, залогодатели, залогодателями по закладной; векселедатели, векселедержатели, лизингополучатели, (представители, правопреемники);
- Физические лица, контрагенты Банка или представляющие интересы контрагентов Банка.

4.2. Обработка персональных данных в Банке осуществляется в целях:

- осуществления банковских операций, оказания финансовых услуг и иной деятельности, предусмотренной Уставом Банка, действующим законодательством Российской Федерации, нормативными актами Банка России;
- осуществления и выполнения, возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей, в том числе предусмотренных международным договором Российской Федерации или законом;
- осуществления организации кадрового учета, включая подбор и оформление кандидатов;
- осуществления Банком административно-хозяйственной деятельности.

4.3. Банк осуществляет обработку персональных данных субъектов персональных данных с использованием средств автоматизации и без использования средств автоматизации.

Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.4. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Банк обеспечивает запись, систематизацию, накопление,хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ, обрабатываемых в следующих информационных системах: ПС «CONTACT», ПС «Золотая Корона», ИБС «БИСквит», АИС «ВЕБС», ДБО «Бифит», 1С: Предприятие – Зарплата и управление персоналом.

5. Порядок и условия обработки персональных данных

5.1. Принципы обработки персональных данных

Обработка персональных данных осуществляется Банком в соответствии со следующими принципами:

- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- обработка персональных данных осуществляется в соответствии с конкретными, заранее определенными и законными целями и производится до момента достижения этих целей;
- объединение баз данных, содержащих персональные данные, цели, обработки которых несовместимы между собой, недопустимо;
- содержание и объем обрабатываемых персональных данных не противоречат заявленнымцелям обработки, не являются избыточными по отношению к ним;
- при обработке персональных данных в Банке обеспечиваются точность, достаточность, актуальность персональных данных по отношению к цепям их обработки за счет применения необходимых мер по удалению или уточнению неполных, или неточных данных;
- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем это необходимо в соответствии с целями их

обработки, если срок хранения персональных данных не установлен федеральным законом, договоров, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не установлено федеральным законом.

5.2. Условия обработки персональных данных

5.2.1 Условия обработки специальных категорий персональных данных

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, Банком не производится.

5.2.2 Условия обработки биометрических персональных данных

Обработка биометрических категорий персональных данных осуществляется Банком при наличии согласия в письменной форме субъекта персональных данных.

Представление биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона «О персональных данных». Банк не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на обработку персональных данных, если в соответствии с Федеральным законом «О персональных данных» получение Оператором согласия на обработку персональных данных не является обязательным.

5.2.3. Условия обработки иных персональных данных

Обработка иных категорий персональных данных осуществляется Банком с соблюдением следующих условий:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения, возложенных законодательством РФ на Банк, полномочий обязанностей;
- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных, или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта

персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных.

5.3. Конфиденциальность персональных данных

5.3.1. Сотрудники Банка, получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональные данных, если иное не предусмотрено федеральным законом.

5.3.2. Банк определяет места хранения отдельных категорий персональных данных (их материальных носителей), обрабатываемых без использования средств автоматизации.

5.3.3. Сохранность персональных данных и исключение несанкционированного доступа к ним обеспечиваются путем:

- хранения документов, в металлических запирающихся шкафах, либо в специально выделенных для хранения помещениях сергламентированным доступом;
- передачей на архивное хранение либо уничтожением документов, содержащих персональные данные, при достижении целей их обработки.

5.3.4. Доступ к информационным системам, содержащим персональные данные, обеспечивается использованием средств защиты от несанкционированного доступа и копирования. Помещения, где осуществляется хранение, и обработка персональных данных отвечают требованиям, обеспечивающим их сохранность в соответствии с законодательством РФ.

5.4. Общедоступные источники персональных данных

5.4.1. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

5.4.2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

5.5. Согласие субъекта персональных данных на обработку его персональных данных

5.5.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным,

информативным, сознательным и однозначным. 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 федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных проверяются Банком.

5.5.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных, Банк вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, предусмотренных частью 2 статьи 9 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

5.5.3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на Банк.

5.5.4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о даче выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование и адрес Оператора;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Банком способов обработки персональных данных;

7) срок, в течение которого действует согласие субъекта персональных данных, а также

способ его отзыва, если иное не установлено федеральным законом;

8) подпись субъекта персональных данных.

5.5.5. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

5.5.6. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

5.6. Трансграничная передача персональных данных

5.6.1. Трансграничная передача персональных данных осуществляется в соответствии с 152-ФЗ «О персональных данных» и международными договорами Российской Федерации.

5.6.2. Трансграничная передача персональных данных осуществляется, как в страны, обеспечивающие адекватную защиту прав субъектов персональных данных, так и в страны, не обеспечивающие адекватную защиту прав субъектов персональных данных в целях осуществления переводов с использованием в платежных системах в рамках заключенных договоров.

5.6.3. Банк до начала осуществления деятельности по трансграничной передаче персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных.

5.7. Обработка персональных данных, осуществляемая без использования средств автоматизации.

5.7.1. Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронные носители информации.

5.7.1.1. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель дня каждой категории персональных данных.

5.7.1.2. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм

(бланков);

• документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

• дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

5.7.1.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных;

б) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

в) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.7.1.4. Неавтоматизированная обработка персональных данных в электронном виде осуществляется с применением организационных и технических мер, исключающих возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

5.7.1.5. При несовместимости целей неавтоматизированной обработки персональных данных (если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных натом же носителе персональных данных), должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия

персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

5.7.1.6. Документы и внешние электронные носители информации, содержание персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

5.7.1.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированныхна материальном носителе (удаление, вымарывание).

6. Обязанности Оператора

6.1. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю Банком при обращении в течение десяти рабочих дней с момента обращения либо при получении запроса субъекта персональных данных или его законного представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Прием и обработка поступающих запросов субъектов персональных данных в Банк осуществляется в соответствии с Инструкцией по делопроизводству, фиксируется запрос в Журнале входящих документов, ответственность за ведение которого лежит на специалисте Общего отдела Банка. Исполнение таких запросов также осуществляется в порядке, установленном Инструкцией по делопроизводству, профильным подразделением Банка, занимающимся обработкой персональных данных.

Срок исполнения запросов – не больше десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Оператором в адрес

субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Оператор предоставляет сведения, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

6.2. Обязанности Оператора

6.2.1. Обязанности Оператора при сборе персональных данных:

6.2.1.1. При сборе персональных данных, Банк предоставляет субъекту персональных данных по его просьбе запрашиваемую информацию, касающуюся обработки его персональных данных в соответствии с частью 7 статьи 14 Федерального закона «О персональных данных».

6.2.1.2. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение Оператором согласия на обработку персональных данных являются обязательными, Банк разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

6.2.2. Меры, направленные на обеспечение выполнения Банком своих обязанностей.

6.2.2.1. Банк принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, если иное не предусмотрено федеральными законами. К таким мерам, в частности, относятся:

1) назначение ответственного за организацию обработки персональных данных;

2) издание Политики, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям к защите персональных данных, Политике, локальным актам Банка;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;

6) ознакомление сотрудников Банка, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, Политикой, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

6.2.3. Меры по обеспечению безопасности персональных данных при их обработке.

6.2.3.1. Банк при обработке персональных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, представления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.2.3.2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением факторов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных

данных и уровня защищенности информационных систем персональных данных;

6.2.4. Обязанности Оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных:

6.2.4.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, Банк осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, Банк осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.2.4.2. В случае подтверждения факта неточности персональных данных, Банк на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные в течении семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.2.4.3. В случае выявления неправомерной обработки персональных данных, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных. В случае если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, не превышающий десяти рабочих днейс даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Банк уведомляет субъекта персональных данных или его представителя, а в случае, если обращения субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.2.4.4. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Банком, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган

по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также о лице, уполномоченном Банком на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также о лицах, действия которых стали причиной выявленного инцидента (при наличии).

6.2.4.5. В случае достижения цели обработки персональных данных Банк прекращает их обработку и уничтожает в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных.

6.2.4.6. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных, Банк прекращает их обработку, и в случае, если сохранение персональных данных более не требуется для целей обработки, они уничтожаются в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

6.2.4.7. В случае обращения субъекта персональных данных с требованием о прекращении обработки персональных данных, Банк в срок, не превышающий десяти рабочих дней с даты получения соответствующего требования, прекращает их обработку, за исключением случаев, предусмотренных пунктами 2-11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банка в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информацию

6.2.4.8. В случае отсутствия возможности уничтожения персональных данных в течении

указанного срока, Банк блокирует такие персональные данные и обеспечивает их уничтожение в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.2.4.9. Уничтожение документов на бумажных носителях, содержащих персональные данные, осуществляется в соответствии с внутренними документами Банка. По итогам уничтожения документов составляется соответствующий акт, утверждаемый лицом, ответственным за соблюдение порядка хранения персональных данных в подразделении.

6.2.4.10. В случае если обработка персональных данных осуществляется Оператором без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

6.2.4.11. В случае если обработка персональных данных осуществляется Оператором с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных (далее – выгрузка из журнала).

6.2.4.12. Акт об уничтожении персональных данных и выгрузка из журнала должны соответствовать Требованиям к подтверждению уничтожения персональных данных, утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 №179.

7. Сферы ответственности

7.1 Лица, ответственные за организацию обработки персональных данных в организациях

7.1.1. Банком назначается лицо ответственное за организацию обработки персональных данных.

7.1.2. Лицо ответственное за организацию обработки персональных данных получает указание непосредственно от исполнительного органа организации, являющейся Оператором, и подотчетно ему.

7.1.3. Банк предоставляет лицу ответственному за организацию обработки персональных, необходимые сведения.

7.1.4. Лицо ответственное за организацию обработки персональных данных, выполняет функции, предусмотренные законодательством Российской Федерации, а также нормативными документами Банка.

7.2. Ответственность

7.2.1. Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

7.2.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом «О персональных данных», а также требований к защите персональных данных, установленных в соответствии с Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

8. Заключительные положения.

8.1. Настоящая Политика является внутренним документом Оператора, общедоступной и подлежит размещению на официальной странице Оператора в сети Интернет.

8.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

8.3. Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности персональных данных Оператора.

8.4. Ответственность должностных лиц Оператора, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними нормативными документами Оператора.