ИНВЕСТИЦИОННЫЙ КОММЕРЧЕСКИЙ БАНК РАЗВИТИЯ «ЯРИНТЕРБАНК»
(ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ)
ИКБР «ЯРИНТЕРБАНК» (ООО)

УТВЕРЖДЕНО
Решением Правления
ИКБР «ЯРИНТЕРБАНК» (ООО)
Протокол от 01.03.2024 № б/н

ПОЛИТИКА
О ПОРЯДКЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ИКБР «ЯРИНТЕРБАНК» (ООО)

г. Ярославль, 2024

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика о порядке обработки персональных данных в ИКБР «ЯРИНТЕРБАНК» (ООО) (далее – Политика) разработана в Инвестиционном коммерческом банке развития «ЯРИНТЕРБАНК» (общество с ограниченной ответственностью) (далее – Банк) в соответствии с:

- Конституцией Российской Федерации;
- Федеральным законом Российской Федерации от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Трудовым кодексом Российской Федерации;
- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Методическими рекомендациями по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации, разработанными совместно Центральным Банком Российской Федерации, Ассоциацией Российских Банков, Ассоциацией региональных банков России (Ассоциация «Россия»);
- Приказом ФСТЭК 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».

1.2. Целью настоящей Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в ИКБР «ЯРИНТЕРБАНК» (ООО), в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайны, а также определение порядка обработки персональных данных субъектов персональных данных, установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.

1.3. Действие настоящего документа распространяется на все процессы, связанные с обработкой персональных данных в Банке.

1.4. Все сотрудники Банка, имеющие доступ к персональным данным субъектов персональных данных, в обязательном порядке должны быть ознакомлены с настоящим Политикой под роспись.

1.5. На основании приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Банк включен в реестр операторов, осуществляющих обработку персональных данных.

1.6. Пересмотр и обновление настоящей Политики осуществляется:

- в случае внесения изменений в законодательство Российской Федерации в области персональных данных, требующих актуализации настоящей Политики;
- по результатам анализа актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности;
- по результатам других контрольных мероприятий.

1.7. Настоящая Политика, определяющая деятельность Банка в отношении обработки и защиты персональных данных, подлежит публикации на официальном сайте Банка www.yarinterbank.ru.

2. ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Для целей настоящей Политики и принимаемых в Банке для ее реализации локальных актов применяются следующие термины и определения:

Автоматизированная обработка персональных данных - обработка персональных данных с использованием средств вычислительной техники.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

Безопасность информации – состояние защищённости информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения, информации, в том числе её передачи.

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

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных (далее - ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Модель угроз – перечень возможных угроз информации.

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

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

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

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Ответственный за организацию обработки персональных данных – должностное лицо, которое назначается приказом Председателя Правления, организующее принятие правовых, организационных и технических мер в целях обеспечения надлежащего выполнения функций по организации обработки персональных данных в Банке в соответствии с положениями законодательства.

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

Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку

персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом № 152-ФЗ.

Персональные данные клиента – любая информация, касающаяся конкретного лица, с которым в установленном законом порядке заключен договор об оказании банковской услуги, и необходимая в целях исполнения договора.

Персональные данные работника – любая информация, касающаяся конкретного лица, с которым в установленном законом порядке заключен трудовой договор, и необходимая Банку в связи с трудовыми отношениями.

Персональные данные кандидата на трудоустройство – любая информация, касающаяся конкретного лица, которое в установленном законом порядке претендует на вступление с Банком в трудовые отношения;.

Персональные данные иного лица – любая информация, касающегося конкретного лица, которое обращается в Банк и предоставляет свои персональные данные в связи с необходимостью принятия решения или совершения каких-либо действий, порождающих юридические последствия в отношении указанного лица или других лиц.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

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

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

Уничтожение информации – действия, в результате которого невозможно восстановить содержание информации в информационной системе или в результате которых уничтожаются материальные носители информации.

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

Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2.2. В Банке обрабатываются персональные данные следующих категорий субъектов персональных данных:

- персональные данные работников, кандидатов на трудоустройство согласно утвержденному Порядку организации работы с персональными данными работников и кандидатов на трудоустройство в ИКБР «ЯРИНТЕРБАНК» (ООО), в котором определяется в том числе цели обработки и перечень обрабатываемых Банком персональных данных работников и кандидатов на трудоустройство и разграничивается уровень доступа сотрудников Банка к таким персональным данным;

- персональные данные клиентов Банка и иных лиц согласно утвержденному Порядку организации работы с персональными данными клиентов ИКБР

«ЯРИНТЕРБАНК» (ООО) и иных лиц, в котором определяется в том числе цели обработки и перечень обрабатываемых Банком персональных данных клиентов Банка, контрагентов и иных лиц и разграничивается уровень доступа сотрудников Банка к таким персональным данным;

- **общедоступные персональные данные контрагентов**, которые не требуют осуществления мероприятий по обеспечению их безопасности.

3. ОБЩИЕ ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных осуществляется на основе следующих принципов:

- законности целей и способов обработки персональных данных;
- добросовестности Банка, как оператора персональных данных, что достигается путем выполнения требований законодательства Российской Федерации в отношении обработки персональных данных;
- соответствия состава и объема обрабатываемых персональных данных, а также способов обработки персональных данных заявленным целям обработки;
- точности и достаточности, а в необходимых случаях и актуальности персональных данных по отношению к заявленным целям их обработки;
- уничтожения персональных данных по достижении целей обработки способом, исключающим возможность их восстановления;
- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.2. Обработка персональных данных при неавтоматизированной их обработке регламентирована Правилами обработки персональных данных без использования средств автоматизации.

Обработка персональных данных при их обработке в ИСПДн регламентирована соответствующими инструкциями администратора безопасности ИСПДн, пользователя ИСПДн и другими внутренними документами Банка по защите информации.

3.3. Работники Банка, допущенные к обработке персональных данных, обязаны:

- знать и неукоснительно выполнять требования настоящей Политики и законодательства Российской Федерации в области персональных данных;
- обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей;
- не запрашивать дополнительную информацию, содержащую персональные данные, за исключением тех сведений, которые необходимы для достижения целей обработки персональных данных;
- соблюдать режим конфиденциальности и не разглашать персональные данные, обрабатываемые в Банке;
- разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не сообщать персональные данные субъектов персональных данных в коммерческих целях без его письменного согласия;
- не сообщать персональные данные субъектов третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъектов, а также в случаях, установленных федеральным законом;
- сообщать о действиях других лиц, которые могут привести к нарушению требований настоящей Политики;
- сообщать об известных фактах нарушения требований настоящей Политики ответственному за организацию обработки персональных данных в Банке.

В целях защиты персональных данных, хранящихся в Банке, работник, осуществляющий обработку персональных данных, имеет право:

- получать и обрабатывать информацию, содержащую персональные данные, в соответствии с его полномочиями;

- требовать оповещения Банком субъекта персональных данных обо всех произведенных в них исключениях, исправлениях или дополнениях.

3.4. Обработка персональных данных осуществляется в Банке с письменного согласия субъекта персональных данных на обработку его персональных данных, форма которого утверждается Председателем Правления ИКБР «ЯРИНТЕРБАНК» (ООО).

3.5. Письменное согласие на обработку персональных данных должно включать в себя:

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

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

- наименование (полное и сокращенное) и адрес Банка;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

- подпись субъекта персональных данных.

3.6. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяется Банком.

3.7. 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 для обработки, предусмотренных законодательством Российской Федерации.

3.8. Согласие субъекта персональных данных не требуется в случаях, установленных федеральным законом. Соблюдение конфиденциальности такой информации является для Банка обязательным.

3.9. В целях обеспечения прав и свобод субъекта персональных данных Банк при обработке персональных данных обязан соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях заключения с Банком договоров и их дальнейшего исполнения, в целях оказания банковских услуг, а также в целях принятия решений, совершения действий или получения информации в отношении субъекта персональных данных;

- все персональные данные субъекта персональных данных Банк должен получать у него самого; если персональные данные субъекта персональных данных возможно получить только у представителя, Банк проверяет полномочия представителя;

- в случае получения сведений, содержащих персональные данные, у третьей стороны, Банк до начала обработки персональных данных предоставляет информацию, предусмотренную частью 3 ст. 18 Федерального закона № 152-ФЗ;

- в случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных;

- 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;

- при определении объема и содержания обрабатываемых персональных данных Банк должен руководствоваться законодательством Российской Федерации; сотрудник Банк, ответственный за совершение банковской операции, принимающий решение, порождающее юридическое последствие, или предоставляющий информацию, определяет объем, содержание обрабатываемых персональных данных, руководствуясь законодательством Российской Федерации и внутренними документами Банка;

- Банк не обрабатывает специальные категории персональных данных субъектов персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

4. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Банк осуществляет обработку персональных данных смешанным путем: с использованием средств автоматизации с соблюдением порядка, предусмотренного Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и без использования средств автоматизации с соблюдением порядка, предусмотренного Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4.2. В Банке запрещается принятие решений на основании исключительно автоматизированной обработки персональных данных, которые порождают юридические последствия в отношении субъекта персональных данных, или иным образом затрагивают его права и законные интересы, кроме случаев и условий, предусмотренных законодательством Российской Федерации в области персональных данных.

4.3. Банк вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, на основании заключаемого с этим лицом договора, условием которого является соблюдение конфиденциальности и неразглашения персональных данных. Поручение на обработку персональных данных должно соответствовать требованиям, установленным Федеральным законом № 152-ФЗ.

4.4. Персональные данные не раскрываются третьим лицам и не распространяются иным образом без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

4.5. Представители органов государственной власти (в том числе контролирующих, надзорных, правоохранительных и иных органов), получают доступ к персональным данным, обрабатываемым в Банке, в объеме и порядке, установленном законодательством Российской Федерации.

5. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Банк, как оператор персональных данных, должен обеспечивать бесплатный доступ субъекта к персональным данным, ему соответствующим.

5.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Банком;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Банком способы обработки персональных данных;
- наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе, сроки их хранения;
- и иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

5.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

5.4. Для получения доступа к своим персональным данным субъекту необходимо направить в Банк запрос, содержащий паспортные данные субъекта персональных данных, в бумажной или электронной форме, подписанные собственноручно или квалифицированной электронной подписью.

5.5. Работники Банка должны предоставить персональные данные субъекту в доступной форме, в которых не должны содержаться персональные данные, относящиеся к другим субъектам.

5.6. Должностные лица Банка, в обязанность которых входит обработка запросов и обращений субъектов персональных данных, обязаны обеспечить всем субъектам возможность ознакомления с документами и материалами, содержащими их персональные данные, если иное не предусмотрено законом, в соответствии с Правилами рассмотрения запросов субъектов персональных данных.

5.7. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. Банк обязан удовлетворить требование субъекта по устранению нарушений обработки персональных данных.

5.7. Обработка запросов и обращений субъектов персональных данных в Банке осуществляется в соответствии с Правилами рассмотрения запросов субъектов персональных данных или их представителей.

5.8. Если субъект персональных данных считает, что Банк осуществляет обработку его персональных данных с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Банка в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

5.9. 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.

6. ПРАВА И ОБЯЗАННОСТИ БАНКА

6.1. Банк имеет право осуществлять обработку персональных данных в законных и обоснованных целях, в том числе предоставлять персональные данные третьим лицам, если на это дано информированное согласие субъекта персональных данных или если это предусмотрено действующим законодательством.

6.2. Если обработка персональных данных субъекта осуществляется Банком с письменного согласия, то при сборе персональных данных Банк обязан по просьбе субъекта предоставить информацию о его правах.

6.3. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Банк обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

6.4. Если персональные данные получены не от субъекта персональных данных, Банк до начала обработки персональных данных обязан предоставить субъекту персональных данных информацию, предусмотренную частью 3 ст. 18 Федерального закона № 152-ФЗ, в том числе информацию о наименовании и месте нахождения Банка, о целях, о правовых основаниях обработки, о перечне персональных данных, о предполагаемых пользователях персональных данных, о правах субъекта персональных данных и источнике получения информации, за исключением случаев, специально предусмотренных федеральным законом.

6.5. Банк обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, возложенных на него законодательством в области персональных данных, в частности:

- назначать ответственного за организацию обработки персональных данных;
- издавать документы, определяющие политику Банка в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, определяющие 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 локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- принимать правовые, организационные и технические меры по обеспечению безопасности персональных данных;
- осуществлять внутренний контроль и внутренний аудит соответствия обработки персональных данных ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Банка в отношении обработки персональных данных, локальным актам Банка;
- осуществлять оценку вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых Банком мер,

направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

- знакомить работников Банка, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Банка в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

6.6. В случае выявления недостоверных персональных данных или неправомерных действий с ними Банк при обращении или по запросу субъекта персональных данных или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, обязан устранить допущенные нарушения, или в случае невозможности устранения, уничтожить персональные данные, а также уведомить о своих действиях субъекта персональных данных или уполномоченный орган.

6.7. В случае предоставления субъектом неполных, устаревших, недостоверных или незаконно полученных персональных данных Банк обязан внести необходимые изменения, уничтожить или заблокировать их, а также уведомить о своих действиях субъекта персональных данных.

6.8. По запросу уполномоченного органа по защите прав субъектов персональных данных Банк обязан предоставить ему необходимую информацию.

6.9. В случае выявления неправомерной обработки персональных данных субъекта или неточных персональных данных Банк обязан осуществить блокирование неправомерно обрабатываемых персональных данных субъекта с момента выявления и на период проверки.

6.10. В случае подтверждения факта неточности персональных данных Банк обязан уточнить персональные данные в течение семи рабочих дней и снять блокирование персональных данных.

6.11. В случае подтверждения факта неправомерной обработки Банк обязан в срок, не превышающий трех рабочих дней с даты выявления, прекратить неправомерную обработку персональных данных. Если прекратить неправомерную обработку не представляется возможным Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки, обязан уничтожить такие персональные данные и уведомить об устранении нарушения субъекта персональных данных.

6.12. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Банк обязан с момента выявления такого инцидента Банком, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить 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, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Банком на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

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

6.13. В случае достижения цели обработки персональных данных или в случае отзыва субъектом персональных данных согласия на обработку Банк обязан в срок, не превышающий тридцати дней, уничтожить персональные данные, если иное не

предусмотрено договором или иным соглашением между Банком и субъектом персональных данных.

6.14. В случае отсутствия возможности уничтожения персональных данных в течение установленного Федеральным законом № 152-ФЗ срока Банк осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.15. Подтверждение уничтожения персональных данных в случаях, предусмотренных пунктами 6.11 и 6.13 настоящей Политики осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.

7. ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ И ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Порядок хранения и использования документов, содержащих персональные данные осуществляется в соответствии с законодательством Российской Федерации в области персональных данных.

7.2. Хранение персональных данных осуществляется на бумажных носителях и в электронном виде.

7.2.1. Персональные данные субъектов персональных данных преимущественно хранятся на бумажных носителях в специально отведенных для них местах. Основными документами, содержащими персональные данные, являются: копии документов, удостоверяющих личность, анкета субъекта персональных данных (в случае если такой документ заполняется), а также договоры банковского счета, вклада, кредитный договор (в том числе договор о предоставлении кредита на условиях овердрафта), договор залога, договор поручительства, договор о выдаче банковской гарантии, кадровые документы и иные документы.

7.2.2. Персональные данные субъектов могут также храниться в электронном виде в персональных компьютерах, подключенных к локальной компьютерной сети. Доступ к электронным базам данных ограничен паролем. Возможна передача персональных данных субъектов персональных данных по внутренней сети Банка с использованием технических и программных средств защиты информации, с доступом для сотрудников, допущенных к работе с персональными данными и только в объеме, необходимом сотрудникам для выполнения своих должностных обязанностей.

7.3. Документы, содержащие персональные данные субъектов, по открытым банковским счетам, по действующим договорам хранятся в специальных металлических шкафах. Хранение закрытых банковских счетов, недействующих договоров, а также документов, оконченных производством, осуществляется в архиве Банка. Текущие документы, содержащие персональные данные, хранятся в служебных помещениях Банка, которые по окончании рабочего дня закрываются на ключ, ставятся на сигнализацию и сдаются под охрану сотрудникам охранного предприятия.

7.4. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

7.5. Хранение документов, содержащих персональные данные субъектов, осуществляется в соответствии с Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утвержден Приказом Росархива от 20.12.2019 № 236), Перечнем документов, образующихся в процессе деятельности кредитных организаций, с указанием сроков их хранения

(утвержден Положением Федерального архивного агентства и Центрального банка Российской Федерации от 12.07.2022 № 1/801-П).

7.6. По истечении установленных сроков хранения документы подлежат уничтожению.

7.7. Передача персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных федеральным законом, не допускается. Данное ограничение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

7.8. Передача персональных данных субъекта в коммерческих целях без его письменного согласия исключается. Обработка персональных данных субъекта в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

7.9. Лица, получившие доступ к персональным данным субъекта, должны быть предупреждены о том, что эти данные могут быть использованы лишь в целях, для которых они переданы, и обязаны соблюдать это правило. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности.

7.10. Прием и рассмотрение запросов субъектов персональных данных или их представителей по вопросам обработки персональных данных осуществляются в соответствии с утвержденными Правилами рассмотрения запросов субъектов персональных данных или их представителей.

7.11. В целях исполнения договора об оказании банковских услуг клиентам по перечислению денежных средств третьим лицам Банк осуществляет трансграничную передачу персональных данных на территорию иностранных государств органам власти иностранного государства, иностранным физическим или юридическим лицам. Решение вопросов обеспечения адекватной защиты прав субъектов персональных данных и обеспечения безопасности их персональных данных при трансграничной передаче реализуется в соответствии с Федеральным законом № 152-ФЗ. Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, осуществляется только при наличии согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных, во исполнение договора, стороной которого является субъект персональных данных, а также в иных случаях и в порядке, предусмотренном в части 4 статьи 12 Федерального закона № 152-ФЗ. Все технические средства обработки персональных данных (рабочие станции и серверы) находятся в пределах Российской Федерации.

8. МЕРЫ БАНКА, НАПРАВЛЕННЫЕ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОБЯЗАННОСТИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Безопасность персональных данных в Банке обеспечивается выполнением согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности персональных данных, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и работы информационных систем персональных данных в случае реализации угроз.

8.2. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

8.3. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

8.4. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

8.5. Защита персональных данных субъекта от неправомерного использования или утраты обеспечивается Банком за счет собственных средств в порядке, установленном федеральным законом.

8.6. Внутренняя защита.

8.6.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, сотрудник Банка, работающий с документами и базами данных.

8.6.2. Для обеспечения внутренней защиты персональных данных субъектов необходимо соблюдать ряд мер:

- ограничение и регламентация действий сотрудников Банка, функциональные обязанности которых требуют конфиденциальных знаний;
- обоснованное распределение информации между сотрудниками;
- знание сотрудником Банка норм законодательства по защите персональных данных;
- наличие необходимых условий для работы с конфиденциальными документами и базами данных;
- наличие пароля доступа к информационной базе, размещенной на электронном носителе.

8.7. Внешняя защита.

8.7.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

8.7.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Банка. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

8.7.3. Для обеспечения внешней защиты персональных данных субъектов необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств.

8.8. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны не разглашать эти данные, которые им стали известны в связи с выполнением ими трудовых обязанностей.

8.9. По возможности персональные данные обезличиваются.

8.10. В Банке принимаются следующие меры по защите персональных данных:

8.10.1. назначается ответственный за организацию обработки персональных данных;

8.10.2. издаются локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и

выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

8.10.3. определяются угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

8.10.4. применяются правовые, организационные и технические меры по обеспечению безопасности персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

8.10.5. проводится оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

8.10.6. проводится восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8.10.7. устанавливаются правила доступа к персональным данным, обрабатываемым в информационной системе, а также проводится регистрация и учет действий, совершаемых с персональными данными в информационной системе персональных данных;

8.10.8. внедряются и применяются средства минимизации полномочий доступа, средства разграничения доступа (идентификация и аутентификация субъектов доступа, ограничения количества неудачных попыток доступа) и другие меры защиты;

8.10.9. работники Банка, непосредственно осуществляющие обработку и организующие защиту персональных данных, ознакамливаются с документами, определяющими политику Банка в отношении обработки персональных данных.

8.11. В Банке регламентирована разрешительная система допуска к персональным данным в соответствии с Порядком предоставления доступа к информационным ресурсам.

Перечень лиц, допущенных к обработке персональных данных, формируется на основании данных, представленных руководителями подразделений, в которых ведется обработка персональных данных, и утверждается Председателем Правления Банка.

Работники Банка должны иметь доступ только к тем персональным данным, которые необходимы им для выполнения своих функциональных обязанностей.

Правила доступа к персональным данным в зависимости от функциональных обязанностей устанавливаются следующими документами:

- Порядок организации работы с персональными данными работников и кандидатов на трудоустройство в ИКБР «ЯРИНТЕРБАНК» (ООО);
- Порядок организации работы с персональными данными клиентов ИКБР «ЯРИНТЕРБАНК» (ООО) и иных лиц;
- приказы и распоряжения Председателя Правления Банка.

8.12. Работники Банка допускаются к обработке персональных данных после ознакомления с настоящим Положением, инструкцией пользователя ИСПДн, а также с иной организационно-распорядительной документацией Банка по защите персональных данных.

8.13. Работники Банка, допущенные к обработке персональных данных, перед началом обработки персональных данных подписывают обязательство о неразглашении персональных данных.

8.14. В случае обнаружения нарушений правил обработки персональных данных Правление Банка и/или администратор безопасности ИСПДн и/или ответственный за организацию обработки персональных данных обязаны приостановить предоставление персональных данных пользователям до выявления и устранения причин нарушений.

8.15. Защита персональных данных при неавтоматизированной их обработке регламентирована Правилами обработки персональных данных без использования средств автоматизации.

8.16. Защита персональных данных при их обработке в ИСПДн регламентирована соответствующими инструкциями администратора безопасности ИСПДн, пользователя ИСПДн и другими внутренними документами Банка по защите информации.

8.17. В Банке разработаны модели угроз ИСПДн и модели нарушителей. Проведена классификация ИСПДн. Для ИСПДн сформировано Техническое задание на систему защиты информации, в котором описаны все организационные и технические меры, которые необходимо осуществить для нейтрализации актуальных угроз и выполнения требований действующего законодательства по защите персональных данных установленного уровня защищенности.

8.18. В Банке проводится внутренняя оценка эффективности принятых мер по защите персональных данных, подтвердившая в целом удовлетворительное состояние системы защиты персональных данных.

9. УНИЧТОЖЕНИЕ, БЛОКИРОВАНИЕ И ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Персональные данные субъектов подлежат уничтожению в порядке и случаях, предусмотренных законодательством Российской Федерации.

9.2. Банк обязан прекратить обработку персональных данных и уничтожить их после достижения цели обработки или в случае отзыва субъектом персональных данных согласия на обработку, за исключением случаев, когда уничтожение противоречит федеральному законодательству, а также уведомить о своих действиях субъекта персональных данных и (или) уполномоченный орган. Во всех случаях предусмотрен срок уничтожения персональных данных – три рабочих дня.

9.3. Уничтожение документов, содержащих персональные данные, осуществляется в порядке, предусмотренном действующим законодательством Российской Федерации. В целях оперативной организации уничтожения персональных данных на бумажных носителях приказом Председателя правления Банка назначается комиссия по уничтожению персональных данных, а также утверждается форма акта уничтожения персональных данных.

9.4. Персональные данные, обрабатываемые в ИСПДн, удаляются путем стирания записи в базах данных администратором информационной безопасности информационной системы по запросу субъекта или при достижении целей обработки персональных данных.

9.5. Временное прекращение операций по обработке персональных данных (блокирование) должно производиться по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

9.6. Обезличивание персональных данных на бумажных носителях осуществляется путем удаления на документе, содержащем персональные данные субъекта, части информации посредством вымарывания.

9.7. Обезличивание персональных данных на электронных носителях осуществляется методом декомпозиции, то есть разделения множества персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств. При этом необрабатываемые персональные данные субъектов становятся недоступными для пользователей.

9.8. Подтверждение уничтожения персональных данных в случаях, предусмотренных пунктами 6.7 и 6.9 настоящей Политики, осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.

10. ОТВЕТСТВЕННОСТЬ

10.1. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных в Банке.

10.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие, получающие и использующие информацию о субъектах персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации, ответственность за нарушение правил обработки и защиты этой информации.

10.3. Работники Банка, получающие доступ к персональным данным, несут персональную ответственность за обеспечение конфиденциальности, предоставленной им информации.

10.4. Работники Банка, получающие для работы документы, содержащие персональные данные, несут персональную ответственность за их сохранность.

10.5. Работники Банка, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность, предусмотренную федеральным законодательством.

10.6. За неисполнение или ненадлежащее исполнение работником Банка по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями, составляющими персональные данные субъекта, Банк может применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

10.7. В случае, если нарушение конфиденциальности, целостности или доступности персональных данных повлекло за собой финансовые потери для Банка, виновные должностные лица обязаны возместить причиненный ущерб.