УТВЕРЖДЕНО
Приказом Председателя Правления
АО КБ «Северный Кредит»
от 14 декабря 2015 года №___

ПОЛОЖЕНИЕ
о порядке обработки персональных данных в АО КБ «Северный Кредит»
(в редакции от 14 декабря 2015 года)

25 апреля 2012 года № 01-10/12

(с изменениями №1 от 23.03.2016, приказ №85 от 23.03.2016)

Вологда
2015

ОГЛАВЛЕНИЕ

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее Положение о порядке обработки персональных данных в АО КБ «Северный Кредит» (далее — Положение) разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных») в редакции Федерального закона от 25 июля 2011 года № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и другими федеральными законами и нормативными правовыми актами Российской Федерации, а также в соответствии с Уставом АО КБ «Северный Кредит» (далее - Банк) и внутренними нормативными документами Банка.

1.2. Действие Положения определяет основные требования к порядку обработки (как с использованием средств автоматизации, так и без использования таковых) и обеспечения безопасности персональных данных работников, клиентов, посетителей и иных субъектов персональных данных (определения терминов «работников», «клиентов», «посетителей» даны в п. 4.2.1 настоящего Положения), а также обязанности работников Банка и порядок взаимодействия структурных подразделений Банка в целях обеспечения указанных требований.

1.3. В случае наличия противоречий норм внутренних нормативных документов Банка с нормами настоящего Положения приоритет будет иметь настоящее Положение.

1.4. Порядок обработки персональных данных работников Банка, регламентируется Положением об организации работы с персональными данными работников Банка.

1.5. Необходимые правовые, организационные и технические меры для защиты персональных данных при их автоматизированной обработке в корпоративной информационной системе Банка и при обработке без использования средств автоматизации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, регламентируются настоящим Положением, Политикой информационной безопасности и другими внутренними нормативными документами Банка.

1.6. Передача персональных данных Банком третьему лицу должна осуществляться с согласия субъекта персональных данных, если иное не предусмотрено действующим законодательством РФ.

При этом в договоре с таким лицом должен содержаться текст, аналогичный по своему смыслу следующему:

«Стороны подтверждают, что обработка персональных данных физических лиц, указанных в настоящем договоре или иных документах, получаемых сторонами в процессе исполнения настоящего договора, осуществляется с согласия таких лиц в целях осуществления прав и законных интересов сторон и не нарушает права и свободы физических лиц, Стороны подтверждают, что физические лица уведомлены надлежащим образом об осуществлении обработки их персональных данных передающей стороной.

Сторона, получившая персональные данные от другой стороны, обязана не раскрывать третьим лицам и не распространять эти персональные данные, если иное не предусмотрено законом».

В соответствии с п. 3.7 ст. 5 Федерального закона от 30.12.2004 № 218-ФЗ «О кредитных историях» информационная часть кредитной истории клиентов Банка может передаваться в бюро кредитных историй без согласия субъекта персональных данных.

1.8. Банк вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том

числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее — Поручение).

Лицо, осуществляющее обработку персональных данных по Поручению, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В Поручении должны быть определены:

а) перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;

б) цели обработки персональных данных;

в) обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;

г) требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом «О персональных данных».

Лицо, осуществляющее обработку персональных данных по Поручению, не обязано получать согласие субъекта персональных данных на обработку его 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 оператора, несет ответственность перед Банком.

Если Банк намерен поручить осуществление обработки персональных данных другому лицу, договор, заключенный с этим лицом должен содержать обязательства лица соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных», соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке. В договоре должны быть определены перечень действий (операций) с персональными данными и цели обработки персональных данных, а также требования к защите персональных данных в соответствии с нормами Федерального закона «О персональных данных».

Аналогичным образом ответственность определяется в случае, когда Банку поручается сторонним оператором персональных данных обработка персональных данных субъектов персональных данных, с которыми у Банка отсутствуют непосредственные правовые отношения. Банк в этом случае выступает в роли лица, осуществляющего обработку персональных данных по Поручению.

1.9. В целях информационного обеспечения клиентов Банка в Банке могут создаваться общедоступные источники персональных данных работников Банка (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, адрес места работы, рабочий номер телефона, рабочий адрес электронной почты, должность и иные персональные данные (в случае необходимости), сообщаемые субъектом персональных данных.

Сведения о субъекте персональных данных исключаются из общедоступных источников персональных данных в случае прекращения между субъектом персональных данных и Банком трудовых правоотношений.

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.

1.10. Порядок обработки информации в системах контроля и управления физическим доступом на территорию (в здания и помещения) Банка, в системах видеонаблюдения, а также порядок обращения с носителями на которых эта информация размещается, устанавливается соответствующими внутренними нормативными документами Банка.

1.11. Оценка вреда, который может быть причинен субъектам персональных данных, обработку персональных данных которых осуществляет Банк, в случае нарушения со стороны Банка требований Федерального закона «О персональных данных», а также соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», осуществляется в соответствии с внутренними нормативными документами Банка.

1.12. В соответствии с требованиями Федерального закона «О персональных данных» настоящее Положение или выписка из него в части вопросов, определяющих политику Банка в отношении обработки персональных данных и о реализуемых общих требованиях к защите персональных данных, размещается на официальном сайте Банка http://www.sevcred.ru для обеспечения неограниченного доступа к нему.

1.13. Положения настоящего документа не распространяются на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов, имеющих статус архивных документов в соответствии с действующим законодательством об архивном деле в РФ.

1.14. Требования, изложенные в Положении, являются обязательными для выполнения всеми работниками Банка и иными лицами, имеющими договорные отношения с Банком, при этом срочность и важность выполняемых ими работ не должны являться основанием для нарушения положений Положения и других документов, регламентирующих в Банке вопросы обработки и защиты персональных данных.

1.15. При необходимости получения Банком персональных данных не от самого субъекта персональных данных, например, при осуществлении сделок с корпоративными клиентами, то в соответствии с Федеральным законом «О персональных данных» (ч. 3 ст. 18) Банк до начала обработки таких персональных данных обязан предоставить этому субъекту персональных данных следующую информацию:

а) наименование и адрес (местонахождение, почтовый адрес) Банка;

б) цель обработки персональных данных и ее правовое основание;

в) предполагаемые пользователи персональных данных;

г) установленные Федеральным законом «О персональных данных» права субъекта персональных данных;

д) источник получения персональных данных.

Банк освобождается от обязанности предоставить субъекту персональных данных указанные выше сведения, в случаях, если:

а) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором (лицом, от которого Банк получил персональные данные);

б) персональные данные получены Банком на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

в) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

г) Банк осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

д) предоставление субъекту персональных данных сведений, указанных в предыдущем абзаце настоящего пункта, нарушает права и законные интересы третьих лиц.

1.16. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Банк обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона «О персональных данных».

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. При разработке Положения учитывались требования следующих федеральных законов, нормативных правовых актов, нормативных актов и стандартов:

- Трудовой кодекс Российской Федерации;
- Федеральный закон «О персональных данных»;
- Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»;
- Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах»;
- Федеральный закон от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)»;
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 30.12.2004 № 218-ФЗ «О кредитных историях»;
- Федеральный закон от 23.12.2003 № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации»;
- Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральный закон от 21.12.2013 № 353-ФЗ «О потребительском кредите (займе)»;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. Постановлением Правительства РФ от 15.09.2008 № 687);
-
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
-
- Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (утв. Приказом Минкомсвязи России от 14.11.2011 № 312);
- Стандарт Банка России СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения;
- Стандарт Банка России СТО БР ИББС-1.1-2007. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности;

- Стандарт Банка России СТО БР ИББС-1.2-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014;
-
- Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации (на основе комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации») (утв. Банком России, АРБ, Ассоциацией региональных банков России (Ассоциация "Россия").

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

3.1. Термины и определения, используемые в Положении:

3.1.1. **Автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники.

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

3.1.3. **Информационная система персональных данных (ИСПДн)** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

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

3.1.6**. 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.

3.1.7. **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».

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

3.1.9. **Предоставление персональных данных —** действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

3.1.10. **Представитель** — лицо, которое наделено правом представлять интересы субъекта персональных данных в силу специального указания закона или лицо, представляющее субъекта персональных данных, действующее

на основании поручения (доверенности или иного документа) удостоверенного (удостоверенной) нотариально, или заверенного (заверенной) способами, приравненными к нотариальному заверению согласно ст. 185.1 ГК РФ (далее — Документ).

3.1.11. **Распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

3.1.12. **Уничтожение персональных данных —** 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.

3.1.13. **Субъект персональных данных** – физическое лицо, определенное или определяемое на основании информации, составляющей персональные данные.

4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. Цели и принципы обработки персональных данных.

4.1.1. Банк осуществляет обработку персональных данных в следующих целях:

а) заключения любых договоров с Банком, в том числе обеспечительных, а также в целях оценки правоспособности/дееспособности, платежеспособности/ кредитоспособности при рассмотрении возможности заключения с субъектом персональных данных договора, в том числе при рассмотрении заявок субъекта персональных данных на предоставление банковских услуг, включая передачу персональных данных третьим лицам в соответствии с действующим законодательством Российской Федерации, в том числе в рамках проверок Банка контролирующими/надзорными органами;

б) исполнения договора, в том числе осуществления банковских операций и предоставления всех видов банковских услуг, исполнения обеспечительных и иных договоров, заключаемых с Банком, заключения Банком сделок уступки прав по договорам и иных сделок Банка с правами требования;

в) оповещения субъекта персональных данных с помощью средств связи об изменениях в продуктовой линейке, новых продуктах, услугах и работе Банка, направления субъекту персональных данных адресных предложений банковских услуг, а также проведения маркетинговых исследований;

г) содействия при трудоустройстве в Банк, организации трудовых отношений в Банке, обучения и должностного роста работников, формирования кадрового резерва, учета результатов исполнения работником своих должностных обязанностей, обеспечения работнику установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, информационного обеспечения работы Банка, заключения и исполнения договоров добровольного страхования, прохождения практики (стажировки) в Банке учащихся образовательных учреждений;

д) обеспечения банковской безопасности, связанной с физическим доступом субъектов персональных данных на территорию, в здания и помещения Банка;

е) статистической обработки информации, при условии обязательного обезличивания персональных данных;

ж) опубликования информации о составе органов управления Банком, об аффилированных и иных лицах, раскрытие информации о которых является обязательным согласно требованиям действующего законодательства и нормативных правовых актов Российской Федерации, а также представления такой информации в виде отчетности в Банк России в соответствии с требованиями федеральных законов и нормативных актов Банка России).

4.1.2. Обработка персональных данных в вышеуказанных целях осуществляется в Банке на основе следующих законодательно определенных принципов:

а) обработка персональных данных должна осуществляться на законной и справедливой основе;

б) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

в) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

г) обработке подлежат только персональные данные, которые отвечают целям их обработки;

д) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

е) при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

ж) хранение персональных данных должно осуществляться 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.

4.2. Категории субъектов персональных данных.

4.2.1. В целях реализации Положения в качестве субъектов персональных данных, персональные данные которых могут обрабатываться в Банке с использованием средств автоматизации или без использования таковых, понимаются нижеперечисленные категории физических лиц, условно именуемые далее:

а) **клиентами**, в состав которых включаются:

- физические лица (заемщики, вкладчики и т.п.) и их Представители (лица, действующие по доверенности физических лиц и др.), имеющие договорные отношения с Банком о предоставлении банковских услуг, их поручители, выгодоприобретатели и т.п., а также потенциальные клиенты на этапе преддоговорных отношений с ними (действий в целях заключения договора);
- руководители, участники (акционеры), бенефициарные владельцы, представители и работники юридических лиц, имеющих договорные отношения с Банком о предоставлении банковских услуг (в т.ч. корреспондентов) Банка или находящихся на этапе преддоговорных отношений с Банком;

б) **работниками**, в состав которых включаются:

- персонал Банка (работники, имеющие трудовые отношения с Банком), кандидаты на работу в Банке и лица, имевшие ранее трудовые отношения с Банком;
- лица, проходящие различного рода практику (стажировку) в Банке.

в) **посетителями**, в состав которых включаются:

- представители (должностные лица) государственных органов законодательной, исполнительной и судебной власти и управления;
- представители общественных организаций, коммерческих и некоммерческих структур и иных объединений (в т.ч. иностранных);

г) **иными субъектами персональных данных**, которые не вошли в вышеперечисленные категории и обработка персональных данных которых не противоречит законодательству РФ, в т.ч.:

- физические лица — векселедатели;
- физические лица, являющиеся первым векселедержателем;
- физические лица, являющиеся должниками по закладной;
- физические лица, являющиеся залогодателями по закладной;
- акционеры Банка;
- члены Совета Директоров Банка;
- члены Правления Банка;
- члены Ревизионной комиссии Банка;
- аффилированные лица Банка;
- лица, сделки с которыми, в соответствии с действующим законодательством Российской Федерации, признается для Банка сделками с заинтересованностью;
- лица, под контролем либо значительным влиянием которых находится Банк; ;
- бенефициарные владельцы Банка;
- связанные с Банком лица;
- инсайдеры (физические лица, упомянутые в ст. 4 Федерального закона от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»);
- физические лица, в том числе индивидуальные предприниматели, руководители, представители и работники юридических лиц и индивидуальных предпринимателей, имеющие (имеющих) договорные отношения с Банком гражданско-правового характера, отличные от отношений, связанных с оказанием банком банковских услуг, и трудовых отношений, или находящихся на преддоговорном этапе установления отношений подобного характера;
- иные физические лица, не вошедшие в вышеуказанные категории.

4.3. Категории обрабатываемых персональных данных.

4.3.1. Все обрабатываемые в Банке Персональные данные должны быть отнесены к одной из следующих категорий:

а) **специальные категории** персональных данных;

б) **биометрические** персональные данные;

в) персональные данные **общей** категории, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным;

г) **обезличенные** и/или **общедоступные** персональные данные.

Вышеуказанные категории персональных данных классифицированы Банком с учетом степени тяжести последствий потери свойств безопасности персональных данных для субъекта персональных данных.

4.3.2. Обработка персональных данных, отнесенных к специальным и биометрическим категориям, может осуществляться в порядке, установленном действующим законодательством Российской Федерации.

4.3.3. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность

(биометрические персональные данные) и которые используются Банком для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона «О персональных данных».

4.3.4. В трудовых договорах с работниками Банка и в договорах гражданско-правового характера с иными лицами, в случае, если эти лица имеют доступ к персональным данным, должны быть предусмотрены условия о неразглашении работниками и иными лицами как охраняемой законом банковской, коммерческой или иной законодательно определенной тайны, имеющей в своем составе персональные данные, так и отдельных категорий персональных данных, не входящих в состав тайн.

4.4. Назначение ответственных лиц.

4.4.1. В Банке распорядительным порядком (приказом) назначается лицо, ответственное за организацию обработки персональных данных, как в информационных системах корпоративной информационной системы Банка, в которых обрабатываются персональные данные, так и при обработке без использования средств автоматизации (далее — Ответственный за организацию обработки персональных данных).

Ответственный за организацию обработки персональных данных получает указания непосредственно от исполнительных органов Банка — коллегиального (Правление Банка) и единоличного (Председатель Правления Банка) и подотчетен им.

Ответственный за организацию обработки персональных данных обязан:

- осуществлять внутренний контроль за соблюдением Банком, как оператором персональных данных, и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников Банка положения законодательства Российской Федерации о персональных данных, внутренних нормативных документов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов;
- осуществлять контроль ведения в Банке Журнала учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных в АО КБ «Северный Кредит» (далее – Журнал учета обращений, Приложение №1);
- обеспечивать ведение и корректировку Списка работников Банка, осуществляющих обработку персональных данных, в том числе в ИСПДн, либо имеющих доступ к персональным данным;
- осуществлять контроль сроков подготовки исполнителями ответов на запросы субъектов персональных данных или уполномоченного органа по защите прав субъектов персональных данных;
- обеспечивать регистрацию ответов на запросы субъектов персональных данных или уполномоченного органа по защите прав субъектов персональных данных;
- выполнять иные обязанности, предусмотренные настоящим Положением, трудовым договором с Ответственным за организацию обработки персональных данных и/или распорядительными актами Председателя Правления или лица, его заменяющего.

На время отсутствия Ответственного за организацию обработки персональных данных его обязанности исполняет работник, замещающий его в

соответствии с распорядительным актом Председателя Правления или лица, его заменяющего.

4.4.2. На Ответственного за организацию обработки персональных данных возлагается задача по организации выполнения законодательных требований при обработке персональных данных в Банке.

4.4.3. Ответственными за организацию выполнения требований внутренних нормативных документов Банка по вопросам обработки персональных данных и их защите в структурных подразделениях, обособленных и внутренних структурных подразделениях Банка являются руководители этих подразделений. На время отсутствия руководителей ответственными являются лица, замещающие их. Руководители обособленных и внутренних структурных подразделениях вправе назначить ответственными за отдельные вопросы по организации обработки персональных данных и их защите иных должностных лиц.

4.4.4. Ответственными за выполнение требований внутренних нормативных документов Банка по вопросам обработки персональных данных и их защите в подразделениях, работники которых в соответствии со своими должностными обязанностями уполномочены обрабатывать персональные данные, являются руководители этих подразделений. На время отсутствия этих руководителей ответственными являются лица, замещающие их.

4.4.5. Ответственными за выполнение требований внутренних нормативных документов Банка по вопросам обработки персональных данных и их защите на своих рабочих местах в рамках определенных соответствующими должностными инструкциями являются лица, уполномоченные в установленном порядке обрабатывать в Банке персональные данные.

4.5. Работники, уполномоченные обрабатывать персональные данные.

4.5.1. Работники, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены с положениями законодательства РФ о персональных данных, в том числе с требованиями к защите персональных данных, настоящим Положением, иными внутренними нормативными документами Банка, определяющими политику в отношении обработки персональных данных, и по вопросам обработки персональных данных.

4.5.2. С работниками, непосредственно осуществляющими обработку персональных данных, должны быть в установленном порядке оформлены обязательства о выполнении требований внутренних нормативных актов Банка по обработке, защите и неразглашении информации ограниченного доступа (в т ч. персональных данных) (далее — Обязательство, Приложение №2 к Положению). В трудовых договорах и должностных инструкциях этих работников должны быть оговорены основные принципы работы с персональными данными.

Эти лица должны быть предупреждены о том, что обрабатываемые ими персональные данные могут быть использованы лишь в целях, установленных законодательством РФ и внутренними нормативными актами Банка, и они имеют право доступа только к тем персональным данным, обработка которых предусмотрена должностными обязанностями.

4.5.3. Обязательство подлежит оформлению со всеми лицами, уполномоченными в Банке обрабатывать персональные данные.

4.5.4. Ответственным за организацию и выполнение процедуры согласно п.п.4.5.1-4.5.3. является работник структурного подразделения Банка, уполномоченный на оформление соответствующих договорных отношений.

4.5.5. В Банке должен быть установлен приказом Председателя Правления (в обособленных подразделениях – приказом руководителя подразделения) перечень работников, осуществляющих обработку персональных данных, в том числе в ИСПДн, либо имеющих доступ к персональным данным. Допускается указание работников в перечне (списке) на ролевой основе в соответствии с занимаемой должностью.

4.6. Сроки обработки и хранения обрабатываемых персональных данных.

4.6.1. Сроки обработки персональных данных, содержащихся в типовых и иных формах, регламентируются действующим законодательством РФ, в том числе Федеральным законом «О персональных данных», и указываются в документах, фиксирующих договорные отношения Банка с субъектами персональных данных, и в согласиях субъектов на обработку их персональных данных.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

4.6.2. Процедура хранения персональных данных в Банке проводится в порядке, который позволяет осуществлять хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок их хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Данный порядок соответствует определенному в ч. 7 ст. 5 Федерального закона «О персональных данных» принципу обработки персональных данных.

4.6.3. Сроки хранения персональных данных в Банке, в общем случае, определяются в соответствии со сроками, установленными приказом Министерства Культуры РФ от 25 августа 2010 года № 558 об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», Перечнем типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения, утвержденный приказом Министерства культуры и массовых коммуникаций Российской Федерации от 31 июля 2007 года № 1182, Постановлением ФКЦБ РФ от 16.07.2003 № 03-33/пс «Об утверждении Положения о порядке и сроках хранения документов акционерных обществ», а также иными требованиями законодательства РФ (по срокам исковой давности, по оформлению трудовых отношений и т.д.), нормативных документов федеральных органов исполнительной власти и Банка России, документов, фиксирующих договорные отношения Банка с субъектами персональных данных, и согласий субъектов на обработку персональных данных.

Сроки хранения персональных данных указываются в документах, подтверждающих получение согласия субъекта персональных данных на обработку его персональных данных или во внутренних нормативных документах Банка.

4.7. Допуск к обработке персональных данных и доступ в помещения.

4.7.1. После выполнения процедур, изложенных в разделе 4.5 Положения, лица, уполномоченные обрабатывать в Банке персональные данные, могут быть допущены к обработке персональных данных, если иные условия начала работы дополнительно не оговорены во внутренних нормативных актах Банка.

4.7.2. Для лиц, обрабатывающих персональные данные с использованием средств автоматизации в соответствии со своими должностными обязанностями или в рамках договорных отношений, отличных от трудовых, допуск производится в соответствии с п.4.5.5, а также иными внутренними нормативными документами Банка.

4.7.3. Допуск в помещения, где происходит обработка персональных данных, осуществляется в порядке, изложенном во внутренних нормативных документах.

5. ПРАВОВЫЕ ПРОЦЕДУРЫ ПО ВЗАИМОДЕЙСТВИЮ БАНКА С СУБЪЕКТАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ГОСУДАРСТВЕННЫМИ ОРГАНАМИ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

5.1. Согласие субъекта персональных данных.

5.1.1. В соответствии с Федеральным законом «О персональных данных» (ч. 1 ст. 9) 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 (далее — Согласие) должно быть конкретным, информированным и сознательным.

Согласие 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 от представителя субъекта персональных данных полномочия данного представителя на дачу Согласия от имени субъекта персональных данных проверяются Банком.

5.1.2. Обработка персональных данных допускается в следующих случаях:

а) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

б) обработка персональных данных необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на Банк как на оператора функций, полномочий и обязанностей;

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

г) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

д) 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 оператором 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;

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

ж) обработка персональных данных необходима для осуществления прав и законных интересов Банка как оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

з) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации, при условии обязательного обезличивания персональных данных;

и) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

к) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

В случаях, предусмотренных действующим законодательством Российской Федерации, 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 действующим законодательством Российской Федерации электронной подписью.

5.1.3. В случае обработки специальных категорий персональных данных, применяются требования, установленные Федеральным законом «О персональных данных».

5.1.4. При необходимости трансграничной передачи персональных данных на территории иностранных государств Банк обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

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

а) наличия Согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

б) предусмотренных международными договорами РФ;

г) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя РФ, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

д) исполнения договора, стороной которого является субъект персональных данных;

е) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

5.1.5. В соответствии с Федеральным законом «О персональных данных» (ч. 4 ст. 9) Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

б) 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 Документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

в) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

г) цель обработки персональных данных;

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

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

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

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

и) подпись субъекта персональных данных.

В случае недееспособности субъекта персональных данных Согласие на обработку его персональных данных дает его Представитель.

В случае смерти субъекта персональных данных Согласие дают наследники субъекта персональных данных, если такое Согласие не было дано субъектом персональных данных при его жизни.

5.1.6. Типовые формы согласия субъекта персональных данных / представителя субъекта персональных данных на обработку персональных данных устанавливаются:

- в отношении работников Банка – Положением об организации работы с персональными данными работников Банка;
- в отношении клиентов Банка – Приложениями №№7 – 19 к настоящему Положению;
- в отношении иных субъектов персональных данных – иными внутренними документами Банка.

Текст согласия может включаться в тексты договоров, заявлений, анкет, получаемых у субъекта персональных данных в письменном виде и остающихся на хранении в Банке.

5.1.7. Клиент Банка (субъект персональных данных) может отозвать свое Согласие. В этом случае Банк вправе продолжить обработку персональных данных без Согласия клиента при наличии оснований, указанных в пункте 5.1.2 (п п. б) — к)) Положения.

Федеральным законом «О персональных данных» (ч. 3 ст. 9) обязанность предоставить доказательство получения Согласия субъекта персональных данных или доказательство наличия оснований, указанных в пункте 5.1.2 (п п. б) — к)) Положения, возлагается на Банк.

В случае отзыва клиентом своего Согласия ему необходимо оформить письменный запрос (далее — Запрос на отзыв) с обязательным указанием фамилии, имени, отчества, адрес места жительства (фактического и по месту регистрации), серии и номера основного документа, удостоверяющего его личность, сведений о дате выдачи указанного документа и выдавшем его органе, подписать его и передать лично или через своего представителя в одно из подразделений Банка. Если Отзыв передается через представителя, то он должен предъявить в подразделении Документ, подтверждающий полномочия этого представителя на право представления соответствующих интересов клиента Банка.

5.1.8. В случае, если персональные данные клиента, указанного в Запросе на отзыв, были ранее собраны только с целью оповещения клиента с помощью средств связи об изменениях в продуктовой линейке, новых продуктах, услугах и работе Банка и направления клиенту адресных предложений банковских услуг, а также проведения маркетинговых исследований, то указанные выше структурные подразделения Банка после получения Запроса на отзыв должны немедленно прекратить (организовать и проконтролировать прекращение, если обработка персональных данных с указанной целью осуществляется другим лицом, действующим по поручению Банка) оповещение клиента и в срок, не превышающий

30 дней с момента поступления Запроса на отзыв, уничтожить (организовать и проконтролировать уничтожение, если обработка персональных данных с указанной целью осуществляется другим лицом, действующим по поручению Банка) персональные данные клиента, отозвавшего свое Согласие, в информационных системах Банка, с помощью которых осуществляется оповещение клиентов.

Банк в соответствии с Федеральным законом «О персональных данных» (ч. 2 ст. 15) обязан немедленно прекратить обработку персональных данных клиента для вышеуказанной цели также по требованию клиента, выраженному в любой форме, в том числе отличной от традиционной письменной на бумажном носителе, например, в форме сообщения, переданному с использованием электронной почты или факса, но не подписанного электронной подписью в соответствии с федеральным законом.

5.1.9. Действия работников Банка по блокированию, уничтожению (обезличиванию) персональных данных клиента (субъекта персональных данных) или его Представителя, а также по их уведомлению о факте уничтожения Банком (лицом, осуществляющим обработку персональных данных по поручению Банка) его персональных данных в соответствии с Федеральным законом «О персональных данных» (ч. 5, ч. 6 ст. 21), в том числе для случая отзыва клиентом своего Согласия, изложены в разделе 5.4 настоящего Положения.

5.1.10. В случае, если персональные данные клиента, указанного в Запросе на отзыв, были ранее собраны не только с целью, указанной в первом абзаце пункта 5.1.8, но и с целью оказания иных услуг на основании договорных отношений с Банком, то указанные выше структурные подразделения Банка после получения Запроса на отзыв должны незамедлительно прекратить (организовать и проконтролировать прекращение, если обработка персональных данных с указанной целью осуществляется другим лицом, действующим по поручению Банка) оповещение клиента без уничтожения его персональных данных, необходимых для выполнения договорных обязательств Банка или требований федеральных законов.

В этом случае основанием для продолжения обработки персональных данных клиента являются условия, указанные в пункте 5.1.2 (п п. б) — к)) настоящего Положения в соответствии с требованиями Федерального закона «О персональных данных» (ч. 2 ст. 9). При этом обязанность доказательства соблюдения указанных условий возлагается законодательством РФ на Банк.

5.1.11. Оригиналы Запросов на отзыв согласий клиента хранятся в сформированном при открытии банковского счета юридическом деле клиента. Срок хранения Запросов на отзыв аналогичен сроку хранения других документов из юридического дела клиента, содержащих его персональные данные.

В случае отсутствия в Банке юридического дела клиента, отзывающего свое Согласие, оригиналы Запросов на отзыв надлежит хранить в отдельном деле «Отзывы согласий на обработку персональных данных субъектов персональных данных», которое ведется в соответствии с утвержденной Номенклатурой дел Банка.

5.2. Доступ субъектов персональных данных к обрабатываемым персональным данным

5.2.1. В соответствии с Федеральным законом «О персональных данных» (ч. 7 ст. 14) субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных Банком;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые Банком способы обработки персональных данных;

г) 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;

д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

е) сроки обработки персональных данных, в том числе сроки их хранения;

ж) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

з) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

л) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

В соответствии с Федеральным законом «О персональных данных» (ч. 1 ст. 20) Банк обязан сообщить в порядке, предусмотренном настоящим разделом Положения, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

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

а) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

б) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством РФ случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

в) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

г) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

д) обработка персональных данных осуществляется в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

5.2.3. Выбор формы обращения (запроса) для реализации своего права на получение сведений зависит от воли субъекта персональных данных. Сведения, указанные в п. 5.2.1 Положения, могут быть предоставлены субъекту персональных данных или его Представителю для ознакомления в случае:

а) устного обращения к работникам Банка, сопровождающегося обязательным предоставлением основного документа, удостоверяющего личность субъекта персональных данных или его представителя, а также Документа, подтверждающего полномочия этого представителя;

б) предоставления запроса в Банк, который может быть исполнен как на бумажном носителе (при личном обращении субъекта или его представителя), так и в форме электронного документа, подписанного электронной подписью в соответствии с законодательство Российской Федерации. Запрос должен содержать: номер основного документа, удостоверяющего личность клиента или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие клиента в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком, подпись клиента или его представителя.

Обращение (запрос) субъекта персональных данных регистрируются в Журнале учета обращений. Ведение Журнала учета обращений осуществляется работником, назначенным приказом Председателя Правления Банка (лица, его замещающего), а в филиалах Банка – приказом руководителя филиала (лица, его замещающего).

Журнал учета обращений ведется в электронном виде, начинается в первый рабочий день года и распечатывается по окончании года в случае наличия зафиксированных обращений субъектов персональных данных либо по запросу контролирующих органов, при этом Журнал нумеруется, брошюруется, скрепляется печатью и подписывается Ответственным за организацию обработки персональных данных.

Хранение Журналов учета обращений на бумажном носителе и оригиналы запросов хранятся у Ответственного за организацию обработки персональных данных в течение одного календарного года, а впоследствии подлежат архивному хранению в соответствии с внутренними документами Банка.

Ответ на запрос должен быть направлен субъекту персональных данных и также зарегистрирован в Журнале учета обращений.

5.2.4. В случае получения запроса от представителя клиента полномочия данного представителя на подачу запроса от имени клиента должны проверяться при приеме запроса.

5.2.5. В соответствии с Федеральным законом «О персональных данных» (ч. 4-6 ст. 14) в случае, если сведения, указанные в п. 5.2.1 Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления клиенту по его запросу, то он вправе обратиться повторно в Банк или направить повторный запрос в целях получения сведений, указанных в п. 5.2.1 Положения, и ознакомления с такими персональными данными не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является клиент.

Клиент вправе обратиться повторно в Банк или направить ему повторный запрос в целях получения сведений, указанных в п. 5.2.1 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного выше в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 5.2.6. настоящего Положения, должен содержать обоснование направления повторного запроса.

Банк вправе отказать клиенту в выполнении повторного запроса, не соответствующего условиям, предусмотренным настоящим пунктом. Такой отказ должен быть мотивированным. При этом в соответствии с Федеральным законом «О персональных данных» обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Банке.

5.2.6. Порядок действий в случае выявления недостоверных персональных данных в ходе обработки обращения или запроса субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных приводится в разделе 5.4 настоящего Положения.

5.2.7. В соответствии с Федеральным законом «О персональных данных» (ч. 4 ст. 20) Банк обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30 дней с даты получения такого запроса.

5.3. Отказ в предоставлении персональных данных.

5.3.1. В соответствии с Федеральным законом «О персональных данных» (ч. 2 ст. 20) в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Банк обязан дать в письменной форме мотивированный ответ (Приложение №3), содержащий ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

5.4. Прекращение обработки, уточнение, блокирование и уничтожение персональных данных.

5.4.1. В соответствии с Федеральным законом «О персональных данных» (ч. 1, ч. 3 ст. 21) 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 обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки.

Решение о блокировании персональных данных соответствующего субъекта персональных данных принимает Ответственный за организацию обработки персональных данных.

Проверку факта неправомерной обработки персональных данных организует Ответственный за организацию обработки персональных данных. О результатах проведенной проверки незамедлительно докладывается Ответственному за организацию обработки персональных данных способом и в форме, им определенной в распоряжении или иным порядком.

5.4.2. В соответствии с Федеральным законом «О персональных данных» (ч. 1, ч. 2 ст. 21) в случае выявления неточных (неполных, устаревших) 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 обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных

осуществляется другим лицом, действующим по поручению Банка) 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.

Решение о блокировании предположительно неточных персональных данных соответствующего субъекта персональных данных принимает Ответственный за организацию обработки персональных данных.

Проверку факта неточности обрабатываемых персональных данных организует Ответственный за организацию обработки персональных данных. Проверка проводится, как правило, с участием членов Рабочей группы (в соответствии с назначенными направлениями их работы) и руководителей подразделений Банка, в которых обрабатываются персональные данные, относящиеся к соответствующему субъекту персональных данных. Результаты проведенной проверки незамедлительно докладываются Ответственному за организацию обработки персональных данных способом и в форме, им определенной в распоряжении или иным порядком.

Если при обращении субъекта персональных данных (его представителя) будут обнаружены неточные (неполные, устаревшие) персональные данные, которые можно в присутствии обратившегося и с его согласия оперативно откорректировать, то действия, приведенные в настоящем пункте, допускается не выполнять.

5.4.3. В соответствии с Федеральным законом «О персональных данных» в случае достижения цели обработки персональных данных (ч. 4 ст. 21) или в случае утраты необходимости в достижении этих целей (ч. 7 ст. 5) Банк обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и уничтожить персональные данные (либо провести обезличивание — ч. 7 ст. 5) или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий 30 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 либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

Процедура уничтожения (обезличивания) персональных данных или обеспечения их уничтожения (обезличивания) выполняется в законодательно установленный срок только в том случае, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных, либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами. Данное условие выполнения процедуры уничтожения проверяется в ходе вышеуказанной проверки. По факту уничтожения оформляется Акт об уничтожении документов, содержащих персональные данные (Приложение №4).

5.4.4. В соответствии с Федеральным законом «О персональных данных» в случае отзыва субъектом персональных данных согласия на обработку его персональных данных (ч. 5 ст. 21) Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и в случае, если

сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий 30 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 либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

Вышеуказанные действия в случае отзыва субъектом персональных данных согласия на обработку его персональных данных работникам Банка выполняются после исполнения организационных процедур, изложенных в п п. 5.1.9-5.1.11 Положения.

5.4.5. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в п п. 5.4.1-5.4.4 Положения, Банк в соответствии с Федеральным законом «О персональных данных» (ч. 6 ст. 21) 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 6 месяцев, если иной срок не установлен федеральными законами.

Факт отсутствия возможности уничтожения персональных данных по различным причинам докладывается работником, являющимся в соответствии с настоящим Положением ответственным за организацию (выполнение) процедуры уничтожения, ответственному за организацию обработки персональных данных, который на основании полученного доклада принимает решение об обеспечении уничтожения персональных данных в срок, установленный федеральными законами

5.4.6. В соответствии с Федеральным законом «О персональных данных» (ч. 3 ст. 20, ч. 3 ст. 21) об устранении допущенных нарушений, в результате которых персональные данные были неполными, неточными или неактуальными и подлежали изменению, или об уничтожении персональных данных (в случае неправомерной обработки персональных данных, т е. когда они являются незаконно полученными или не являются необходимыми для заявленной цели обработки), Банк обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение 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.

5.4.7. Банк также обязан принять разумные меры для уведомления третьих лиц, которым были переданы персональные данные субъекта персональных данных в случае, когда с целью устранения допущенных нарушений было необходимо обеспечить изменение переданных персональных данных ввиду их неполноты, неточности или неактуальности. Решение о конкретном составе таких мер и об их исполнении принимает подразделение Банка, установившее от лица Банка соответствующие договорные отношения с указанных третьим лицом. Решение должно быть согласовано с Ответственным за организацию обработки персональных данных.

5.5. Уведомление об обработке персональных данных.

5.5.1. Банк обязан уведомить уполномоченный орган по защите прав субъектов персональных данных об осуществлении обработки персональных

данных в соответствии с требованиями Федерального закона «О персональных данных».

5.5.2. Уведомление об обработке персональных данных должно быть направлено в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом.

Уведомление должно содержать следующие сведения:

а) фирменное наименование, местонахождение Банка;

б) цель обработки персональных данных;

в) категории персональных данных;

г) категории субъектов, персональные данные которых обрабатываются;

д) правовое основание обработки персональных данных;

е) перечень действий с персональными данными, общее описание используемых Банком способов обработки персональных данных;

ж) описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

з) фамилия, имя, отчество физического лица, ответственного за организацию обработки персональных данных Банка, и номера его контактных телефонов, почтовые адреса и адреса электронной почты;

и) дата начала обработки персональных данных;

к) срок или условие прекращения обработки персональных данных.

Уполномоченный орган по защите прав субъектов персональных данных в течение 30 дней с даты поступления уведомления об обработке персональных данных вносит вышеуказанные сведения, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными и публикуются на официальном сайте уполномоченного органа по защите прав субъектов персональных данных в глобальной сети Интернет.

5.5.3. При подготовке уведомления (изменений в уведомление) необходимо руководствоваться официальными рекомендациями уполномоченного органа по защите прав субъектов персональных данных по заполнению образца формы уведомления об обработке персональных данных.

В случае предоставления Банком неполных или недостоверных сведений, указанных в п. 5.5.2 Положения, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от Банка уточнения предоставленных сведений до их внесения в реестр операторов.

5.5.4. В соответствии с Федеральным законом «О персональных данных» (ч. 7 ст. 22) в случае изменения сведений, указанных в уведомлении, Банк обязан уведомить об изменениях уполномоченный орган по защите прав субъектов персональных данных в течение 10 рабочих дней с даты возникновения таких изменений.

5.5.5. Необходимость внесения изменений в ранее поданное уведомление в уполномоченный орган по защите прав субъектов персональных данных определяет Ответственный за организацию обработки персональных данных.

Окончательное решение о внесении изменений в ранее поданное Банком уведомление и о пересылке изменений в уполномоченный орган по защите прав субъектов персональных данных может оформляться распорядительным порядком (приказом или распоряжением по Банку).

5.6. Государственный контроль (надзор) за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных

5.6.1. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием

обработки персональных данных требованиям Федерального закона «О персональных данных», является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи, а именно Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России).

5.6.2. Мероприятия по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных проводятся на основании распоряжения или приказа начальника Центра ФСБ России либо лица его замещающего в соответствии с положениями утвержденного в установленном порядке регламента.

При проведении проверки должностные лица Центра ФСБ России вправе допускаться к средствам криптографической защиты информации (далее — СКЗИ), техническим средствам, на которых они реализованы, оборудованию комплексов, в помещения, в которых установлены СКЗИ, к средствам технической защиты, предназначенным для хранения, обработки и передачи персональных, и ключевых документов.

5.6.3. Контроль и надзор за выполнением требований, установленных Правительством РФ в соответствии с Федеральным законом «О персональных данных», к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

6. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

6.1. Порядок обработки персональных данных, осуществляемой без использования средств автоматизации, строится на принципах, изложенных в Положении об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденном Постановлением Правительства РФ от 15.09.2008 № 687.

6.2. В части совместимости целей обработки персональных данных в Банке устанавливается следующее:

а) цели обработки персональных данных, указанные в подпунктах а), б) и в) пункта 4.1.1 Положения, являются совместимыми;

б) каждая из целей обработки персональных данных, указанная соответственно в подпунктах г), д), е) и ж) пункта 4.1.1 настоящего Положения, не совместима ни с одной другой целью обработки персональных данных.

6.3. При разработке типовых форм, содержащих персональные данные, ответственные за разработку этих форм подразделения Банка должны учитывать следующие положения:

а) фиксация на одном материальном носителе персональных данных субъекта, цели обработки которых несовместимы, не допускается (типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых несовместимы);

б) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать следующие сведения — цель обработки персональных данных, имя (наименование) и адрес Банка, Ф.И.О. 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 и общее описание используемых Банком способов обработки персональных данных;

в) в случаях необходимости получения письменного согласия субъекта на обработку его персональных данных типовая форма должна предусматривать поле, в котором субъект персональных данных может собственноручно поставить отметку о своем согласии на обработку персональных данных: «согласен/не согласен»;

г) 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.

6.4. В случае принятия Банком решения о необходимости ведения журналов (реестров, книг), содержащих персональные данные, используемые для однократного пропуска субъекта персональных данных на территорию (в здания и помещения), на которой размещаются подразделения Банка, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна определяться соответствующим внутренним нормативным документом Банка, в котором должны содержаться сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию (в здания и помещения), на которой находится подразделение Банка, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию (в здания и помещения), на которой находится подразделение Банка.

6.5. Для решения задачи обеспечения безопасности Банка, связанной с физическим доступом субъектов персональных данных (клиентов, посетителей, работников, иных субъектов персональных данных) на территорию Банка, в здания Банка и помещения Банка, в которых осуществляется обработка персональных данных, возможно применение системы видеонаблюдения. При этом материалы видеозаписи системы видеонаблюдения не являются биометрическими персональными данными, поскольку технические характеристики применяемого оборудования не позволяют получать видеозаписи с привязкой к конкретному физическому лицу и использоваться в Банке для установления личности субъекта персональных данных.

6.6. Внутренними нормативными документами Банка определяется порядок не архивного хранения документов (материальных носителей), содержащих персональные данные, который предусматривает раздельное, по возможности, хранение документов по соответствующим категориям персональных данных и по целям их обработки, с назначением мест хранения и ответственных

за хранение с соблюдением конфиденциальности персональных данных и исключением несанкционированного доступа к ним, а также определением мер контроля обеспечения безопасности персональных данных при хранении их материальных носителей.

6.7. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том 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.

6.8. 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, зафиксированных на материальном носителе (удаление, вымарывание).

6.9. Правила, предусмотренные пунктами 6.7 и 6.8 Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

6.10. При необходимости уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, — путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

7. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

7.1. Обеспечение безопасности персональных данных при их обработке с использованием средств автоматизации должно производиться в соответствии с Федеральным законом «О персональных данных» и требованиями, изложенными в подзаконных актах, принятых во исполнение указанного закона.

7.2. Автоматизированные банковские технологические процессы, в рамках которых обрабатываются персональные данные в корпоративной информационной системе Банка, должны быть документированы.

7.3. В Банке должны быть установлены критерии отнесения автоматизированной банковской системы к ИСПДн.

7.4. Для каждой ИСПДн должны быть определены и зафиксированы:

- цели обработки ПДн;
- сроки хранения ПДн и условий прекращения их обработки;

- категории обрабатываемых ПДн (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн);
- процедур учета количества субъектов ПДн, в том числе субъектов ПДн, не являющихся работниками Банка;
- ограничения обработки ПДн достижением цели обработки ПДн;
- соответствие содержания и объема обрабатываемых ПДн установленным целям обработки;
- процедуры получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона “О персональных данных”;
- процедур получения согласия субъектов ПДн на передачу обработки их ПДн третьим лицам, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона “О персональных данных”;
- условия прекращения обработки ПДн и уничтожение либо обезличивание ПДн по достижении целей обработки, по требованию субъекта ПДн в случаях, предусмотренных Федеральным законом “О персональных данных”, в том числе при отзыве субъектом ПДн согласия на обработку ПДн.

7.5. На основе перечисленных в п 4.3.1. категорий персональных данных и в соответствии с требованиями Постановления Правительства №1119 от 01.11.2012 года определяется тип ИСПДн:

7.6. Список информационных систем, содержащих персональные данные, фиксируется в списке, утвержденном приказом Председателя Правления. Списки ИСПДн фиксируется в Акте классификации, утвержденном приказом Председателем Правления.

7.7. Требования к обеспечению безопасности персональных данных для ИСПДн определяются в соответствии с требованиями Постановления Правительства №1119 от 01.11.2012 года.

7.8. Необходимость использования средств криптографической защиты информации или шифровальных (криптографических) средств (далее — СКЗИ), предназначенных для защиты персональных данных при их обработке, хранении и передаче по каналам связи определяется Банком самостоятельно, если иное не предусмотрено законодательством РФ.

7.9. С целью понижения уровня требований по обеспечению безопасности персональных данных, обрабатываемых в ИСПД Банка, рекомендуется проводить процедуру обезличивания персональных данных, т е. действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

7.10. При обработке персональных данных в ИСПД с целью обеспечения безопасности персональных данных при наличии технической возможности рекомендуется:

а) исключать фиксацию на одном материальном носителе и персональных данных, и иных видов информационных активов, а также персональных данных, цели обработки которых заведомо несовместимы;

б) для каждой категории персональных данных использовать отдельный материальный носитель.

8. ОЦЕНКА СООТВЕТСТВИЯ ПОЛОЖЕНИЯМ КОМПЛЕКСА СТАНДАРТОВ БАНКА РОССИИ СТО БР ИББС

8.1. Оценка соответствия положениям стандартов Банка России проводится в следующих формах:

а) оценка соответствия Банка положениям стандарта Банка России СТО БР ИББС-1.0 внешней организацией, имеющей соответствующую аккредитацию Банка России (внешний аудит);

б) самооценка соответствия Банка положениям стандарта Банка России СТО БР ИББС-1.0, проводимая соответствующим подразделением Службы информационной безопасности Банка.

8.2. В качестве внешних проверяющих организаций (внешний аудит) Банком России рекомендуется привлекать организации, имеющие опыт проведения аудита информационной безопасности и оценки соответствия требованиям стандарта Банка России СТО БР ИББС-1.0.-2014

8.3. Самооценка соответствия Банка положениям стандарта Банка России СТО БР ИББС-1.0 проводится по указанию Руководства Банка.

Порядок проведения самооценки в Банке определен в рекомендациях в области стандартизации Банка России РС БР ИББС-2.1.-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0.-204».

В процессе самооценки проводится оценка степени выполнения требований комплекса стандартов Банка России и на ее основе вычисление итогового уровня информационной безопасности Банка. Порядок проведения указанной деятельности (оценка и вычисление) регламентируется стандартом Банка России СТО БР ИББС-1.2.-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».

8.4. Периодичность проведения аудита с целью контроля выполнения требований комплекса стандартов Банка России в части требований по обработке и обеспечению безопасности персональных данных, а также порядок информирования о результатах указанного аудита определяются Банком России совместно с надзорными органами, осуществляющими контроль и надзор в сфере персональных данных (Регуляторами).

8.5. После получения от Банка Подтверждения соответствия Регуляторы при осуществлении надзора (контроля) за выполнением требований законодательства в области персональных данных будут руководствоваться законодательными нормами прямого действия Федерального закона «О персональных данных», соответствующими ведомственными административными регламентами и могут проверить достоверность результатов аудита с использованием стандарта Банка России «СТО БР ИББС-1.2.-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.-2014» в части, касающейся вопросов обработки и безопасности персональных данных.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Банк, его работники, уполномоченные обрабатывать персональные данные, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством РФ ответственность.

9.2. Если субъект персональных данных считает, что Банк как оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, то он вправе обжаловать действия или бездействие Банка

в уполномоченный орган по защите прав субъектов персональных данных 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.

9.3. Банк не несет гражданско-правовую ответственность за распространение информации ограниченной или запрещенной к распространению федеральными законами, если он действует как лицо, оказывающее услуги: либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений; либо по хранению информации и обеспечению доступа к ней при условии, что Банк не мог знать о незаконности распространения информации.

9.4. Банк, как лицо, права и законные интересы которого были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, защите деловой репутации.

Требование о возмещении убытков не может быть удовлетворено в случае, если Банк не принимал мер по соблюдению конфиденциальности информации или нарушил установленные законодательством РФ требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями Банка.

9.5. Все работники Банка, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной ответственности в порядке, установленном Трудовым кодексом РФ.

9.6. Лица, виновные в нарушении требований Федерального закона «О персональных данных», требований Положения несут ответственность, предусмотренную действующим законодательством (гражданско-правовую, административную, уголовную).