УТВЕРЖДЕНО
Наблюдательным советом
АО КБ «КОСМОС»
Протокол № НС-01.09
от «01» сентября 2022 г.

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АО КБ «КОСМОС»

Москва, 2022 г.

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика в отношении обработки персональных данных в АО КБ «КОСМОС» (далее – Политика) определяет принципы, порядок и условия обработки персональных данных работников Банка, иных физических лиц, чьи персональные данные обрабатываются Банком при осуществлении банковской деятельности, а также устанавливает ответственность работников Банка, имеющих доступ к персональным данным, за невыполнение требований норм законодательства Российской Федерации и внутренних нормативных документов Банка, регулирующих обработку и защиту персональных данных, и применяется в отношении всех персональных данных, обрабатываемых в АО КБ «КОСМОС».

1.2. Политика разработана в соответствии с требованиями законодательства Российской Федерации, в том числе:

- Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- Федерального закона от 30.12.2004 № 218-ФЗ «О кредитных историях»;
- Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» (далее – Федеральный закон № 395-1);
- Распоряжением Банка России от 17.05.2014 № Р-399 «Стандарт Банка России «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» СТО БР ИББС-1.2-2014»;
- Распоряжением Банка России от 17.05.2014 № Р-399 «Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014».

1.3. Термины и определения, используемые в Политике:

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

Банк – АО КБ «КОСМОС».

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

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

Клиент - физическое или юридическое лицо, находящееся на обслуживании в Банке, который осуществляет банковские операции, предусмотренные ст. 5 и ст. 6 Федерального закона № 395-1.

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

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор персональных данных (оператор) – АО КБ «КОСМОС», юридическое 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.

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

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

Представитель Клиента - лицо, совершающее сделку от имени и по поручению другого лица (представляемого, доверителя) в силу полномочия, основанного на доверенности, указании закона либо акте уполномоченного на то государственного органа или органа местного самоуправления, к которому относятся:

- любое физическое или юридическое лицо, действующее от имени и по поручению Клиента на основании доверенности;
- физическое лицо, действующее от имени и по поручению Клиента в силу закона или учредительных документов (единоличный исполнительный орган юридического лица, родители, должностные лица органов опеки и т.п.).

Работник – физическое лицо, с которым Банком заключен трудовой договор на выполнение определенных должностных обязанностей.

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

Субъект персональных данных – физическое лицо, в отношении которого Банком провидится обработка его персональных данных.

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

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

1.4. Банк в соответствии с Федеральным законом № 152-ФЗ является оператором, организующим и осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных.

1.5. При определении объема и содержания, обрабатываемых Банком персональных данных, Банк руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами Российской Федерации, нормативными актами Банка России и внутренними нормативными документами Банка.

1.6. Положения Политики распространяются на отношения по обработке и защите персональных данных, полученных Банком как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите персональных данных, полученных до ее утверждения.

1.7. Во исполнение требований ч. 2 ст. 18.1 Федерального закона № 152-ФЗ Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте Банка.

1.8. Если в отношениях с Банком участвуют наследники (правопреемники) и (или) представители субъектов персональных данных, то Банк становится оператором персональных данных лиц, представляющих указанных субъектов.

Положения Политики и другие внутренние нормативные документы Банка распространяются на случаи обработки и защиты персональных данных наследников (правопреемников) и (или) представителей субъектов персональных данных, даже если эти лица во внутренних нормативных документах Банка прямо не упоминаются, но фактически участвуют в правоотношениях с Банком.

2. ПРИНЦИПЫ И ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Принципы обработки персональных данных.

Для обеспечения безопасности персональных данных Банк руководствуется следующими принципами:

1) **законность**: защита персональных данных основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты персональных данных;

2) **системность**: обработка персональных данных в Банке осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных;

3) **комплексность**: защита персональных данных строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Банка (далее - ИС) и других имеющихся в Банке систем и средств защиты;

4) **непрерывность**: защита персональных данных обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки персональных данных, в том числе при проведении ремонтных и регламентных работ;

5) **своевременность**: меры, обеспечивающие надлежащий уровень безопасности персональных данных, принимаются до начала их обработки;

6) **преемственность и непрерывность совершенствования**: модернизация и наращивание мер и средств защиты персональных данных осуществляется на основании результатов анализа практики обработки персональных данных в Банке с учетом выявления новых способов и средств реализации угроз безопасности персональных данных, отечественного и зарубежного опыта в сфере защиты информации;

7) **персональная ответственность**: ответственность за обеспечение безопасности персональных данных возлагается на Работников Банка в пределах их обязанностей, связанных с обработкой и защитой персональных данных;

8) **минимизация прав доступа**: доступ к персональным данным предоставляется Работникам Банка только в объеме, необходимом для выполнения их должностных обязанностей;

9) **гибкость**: обеспечение выполнения функций защиты персональных данных при изменении характеристик функционирования ИСПДн, а также объема и состава обрабатываемых персональных данных;

10) **открытость алгоритмов и механизмов защиты**: структура, технологии и алгоритмы функционирования системы защиты персональных данных Банка (далее - СЗПДн) не дают возможности преодоления имеющихся в Банке систем защиты возможными нарушителями безопасности персональных данных;

11) **научная обоснованность и техническая реализуемость**: уровень мер по защите персональных данных определяется современным уровнем развития информационных технологий и средств защиты информации;

12) **специализация и профессионализм**: реализация мер по обеспечению безопасности персональных данных и эксплуатация СЗПДн осуществляются Работниками Банка, имеющими необходимые для этого квалификацию и опыт;

13) **эффективность процедур отбора кадров и выбора контрагентов**: кадровая политика Банка предусматривает тщательный подбор персонала и мотивацию Работников Банка, позволяющую исключить или минимизировать возможность нарушения ими безопасности персональных данных; минимизация вероятности возникновения угрозы безопасности персональных данных, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Банка до заключения договоров;

14) **наблюдаемость и прозрачность**: меры по обеспечению безопасности персональных данных должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

15) **непрерывность контроля и оценки**: устанавливаются процедуры постоянного контроля использования систем обработки и защиты персональных данных, а результаты контроля регулярно анализируются.

2.1.1. Обработка персональных данных в Банке ограничивается достижением Банком конкретных, заранее определенных и законных целей.

2.1.2. Обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Персональные данные обрабатываются в Банке в целях:

- обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- осуществления возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: "О банках и банковской деятельности", "О кредитных историях", "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма", "О валютном регулировании и валютном контроле", "О рынке ценных бумаг", "О несостоятельности (банкротстве) кредитных организаций", "О страховании вкладов физических лиц в банках Российской Федерации", "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования", "О персональных данных", нормативными актами Банка России, а также Уставом и нормативными документами Банка;
- заключения, исполнения, прекращения гражданско-правовых договоров с Клиентами/контрагентами Банка в соответствии с законодательством Российской Федерации;
- организации кадрового учета Банка, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам; ведения кадрового делопроизводства, содействия Работникам в обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечения, заполнения первичной статистической документации, в соответствии с законодательством Российской Федерации, Уставом и внутренним нормативными документами Банка;
- рассмотрения обращений граждан;
- привлечения и отбора кандидатов на работу в Банк;
- прием и отправка корреспонденции;
- обеспечения пропускного режима на объектах Банка.

3. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъект персональных данных имеет право:

3.1. На получение при обращении либо при направлении письменного запроса Субъекта персональных данных или его представителя информации, касающейся обработки его персональных данных, в том числе содержащую:

1) подтверждение факта обработки персональных данных Банком;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Банком способы обработки персональных данных;

4) наименование и место нахождения Банка, сведения о юридических и физических 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 № 152-ФЗ;

5) обрабатываемые персональные данные, относящиеся к соответствующему Субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;

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

7) порядок осуществления Субъектом персональных прав, предусмотренных Политикой и Федеральным законом № 152-ФЗ;

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

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

9.1) информацию о способах исполнения Банком обязанностей, установленных статьей 18.1 настоящего Федерального закона;

10) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или иными федеральными законами Российской Федерации.

3.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

3.3. На определение своих представителей для защиты своих персональных данных.

3.4. На требование об уточнении его персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

3.5. На требование о прекращении обработки своих персональных данных, осуществляемой в целях прямого маркетинга.

3.6. На отзыв согласия на обработку персональных данных.

3.7. На обжалование действий или бездействий Банка в уполномоченном органе по защите прав Субъектов персональных данных или в судебном порядке.

3.8. На защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4. ОБЯЗАННОСТЬ БАНКА КАК ОПЕРАТОРА ОСУЩЕСТВЛЯЮЩИМ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Банк обязан:

- использовать полученную информацию исключительно для целей, указанных в Политике;
- обеспечить хранение конфиденциальной информации в тайне, не разглашать без предварительного письменного разрешения Субъекта персональных данных, а также не осуществлять продажу, обмен, опубликование, либо разглашение иными возможными способами переданных персональных данных субъекта, за исключением предусмотренных Политикой и Федеральным законом № 152-ФЗ;
- принимать меры необходимые и достаточные для обеспечения защиты конфиденциальности персональных данных субъекту согласно порядку, используемому в целях информационной безопасности;
- осуществить блокирование персональных данных, относящихся к соответствующему субъекту, с момента обращения или запроса субъекта или его законного представителя либо

уполномоченного органа по защите прав субъектов персональных данных на период проверки, в случае выявления недостоверных персональных данных или неправомерных действий.

5. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Перечень получаемых Банком персональных данных, подлежащих защите в Банке, зависит от цели обработки персональных данных.

Перечень персональных данных, обрабатываемых в Банке, утверждается организационно-распорядительным документом Банка.

5.2. В зависимости от Субъекта персональных данных, Банк получает и обрабатывает следующие категории персональных данных:

5.2.1. Персональные данные Работника Банка – информация, необходимая Банку в связи с заключаемым и/или заключенным трудовым договором и касающаяся конкретного Работника Банка;

5.2.2. Персональные данные акционеров Банка, аффилированных лиц Банка и/или работников юридических лиц, являющихся аффинированными лицами Банка и/или лиц, оказывающих существенное влияние - информация необходимая Банку для отражения в отчетных документах о деятельности Банка в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России и внутренних нормативных документов Банка;

5.2.3. Персональные данные Клиента/контрагента, персональные данные представителей Клиента/контрагента - информация, необходимая Банку для выполнения банковской деятельности, в том числе для выполнения своих обязательств в рамках договорных отношений с Клиентом/контрагентом, и для выполнения требований законодательства Российской Федерации, нормативных актов Банка России и внутренних нормативных документов Банка.

5.2.4. Персональные данные иных лиц, в том числе посетителей Банка.

6. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных в Банке осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ и Политикой.

6.2. **Уведомление Уполномоченного органа по защите прав субъектов персональных данных о начале обработки персональных данных**.

6.2.1. Банк до начала обработки персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев обработки персональных данных:

- включенных в государственные ИСПДн, созданные в целях защиты безопасности государства и общественного порядка;
- в случае, если банк осуществляет деятельность по обработке персональных данных исключительно без использования средств автоматизации.

6.2.2. Уведомление о намерении осуществлять обработку персональных данных (далее – Уведомление) составляется в произвольной форме с учетом обязательных сведений, установленных п.3 ст.22 Федерального закона № 152-ФЗ. В случае направления Уведомления в виде:

- документа на бумажном носителе, подписывается уполномоченным лицом Банка и заверяется печатью Банка или
- электронного документа, подписывается электронной подписью в соответствии с требованиями законодательства Российской Федерации.

6.2.3. В случае изменения сведений, указанных в Уведомлении, а также в случае прекращения обработки персональных данных Банк уведомляет об этом уполномоченный орган по защите прав субъектов персональных данных в течение 10 (десяти) рабочих дней с

даты возникновения таких изменений или с даты прекращения обработки персональных данных.

6.3. В Банке организационно-распорядительным документом назначается Ответственное лицо за организацию обработки персональных данных в Банке.

Лицо, ответственное за организацию обработки персональных данных, обязано:

1) осуществлять внутренний контроль за соблюдением Банком и его работниками требований законодательства Российской Федерации о персональных данных, в том числе требований к их защите, а также соблюдения процедур, установленных внутренними нормативными документами Банка в области защиты персональных данных;

2) доводить до сведения работников Банка положения законодательства Российской Федерации о персональных данных, внутренних нормативных документов Банка по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов Субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

Перечень лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных в Банке, утверждается Приказом Председателя Правления Банка.

6.4. Обработка персональных данных в Банке осуществляется в следующих случаях:

1) обработка персональных данных осуществляется с письменного согласия Субъекта персональных данных на обработку его персональных данных по утвержденной Банком форме;

2) обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей;

3) обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

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

4) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект персональных данных, а также для заключения договора по инициативе Субъекта персональных данных или договора, по которому Субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с Субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы Субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие Субъекта персональных данных;

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

6) обработка персональных данных необходима для осуществления прав и законных интересов Банка или третьих лиц при условии, что при этом не нарушаются права и свободы Субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации.

6.5. Банк вправе поручить обработку персональных данных третьим лицам в случаях оправданной необходимости и с согласия Субъекта персональных данных, если иное не предусмотрено Федеральным законом № 152-ФЗ.

Банк предпринимает все необходимые меры к обеспечению привлеченным к обработке персональных данных третьим лицом соблюдения принципов и правил обработки персональных данных, предусмотренных Политикой и Федеральным законом № 152-ФЗ.

Банк прекращает отношения с третьим лицом в случае систематического или грубого нарушения последним требований Политикой и/или Федерального закона № 152-ФЗ.

6.6. Запись телефонных переговоров с Клиентом осуществляется Банком только при наличии действительной необходимости и не имеет иных целей, кроме:

1) обеспечение Банку возможности подтверждения совершения Клиентом операции;

2) оценки качества услуг Банка по телефону.

Банк в обязательном порядке информирует Клиентов об осуществлении записи до начала телефонного разговора.

6.7. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях в соответствии с требованиями законодательства Российской Федерации и внутренних нормативных документов Банка.

7. СПОСОБЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях исполнения требований законодательства Российской Федерации Банк осуществляет обработку персональных данных следующими способами:

1) Автоматизированную обработку персональных данных - с использованием программно-технических средств, баз данных, информационных технологий и технических средств;

2) Неавтоматизированную обработку персональных данных с использованием бумажного документооборота.

7.2. Принятие решений, порождающих юридические последствия в отношении Субъекта персональных данных или иным образом затрагивающих его права и законные интересы, осуществляется Банком на основании исключительно автоматизированной обработки его персональных данных и только при наличии согласия в письменной форме Субъекта персональных данных.

8. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Порядок обработки персональных данных субъекта персональных данных.

8.1.1. Субъект персональных данных принимает решение о предоставлении его персональных данных, а в случаях, предусмотренных Федеральным законом № 152-ФЗ, дает согласие на их обработку своих персональных данных. Субъект персональных данных принимает решение и дает согласие свободно, своей волей и в своем интересе.

Документами, содержащие письменные согласия субъектов персональных данных на обработку их персональных данных в Банке являются:

- типовая форма согласия субъекта персональных данных на обработку персональных данных представлена в Приложении № 1 к Политике,
- Договор банковского счета,
- Договор срочного банковского вклада;
- Договор аренды индивидуального банковского сейфа;
- Кредитный договор.

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Банком.

8.1.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

В случае отзыва субъектом персональных данных согласия на обработку персональных данных Банк вправе продолжить обработку персональных данных без согласия субъекта

персональных данных при наличии оснований, предусмотренных законодательством Российской Федерации и Политикой.

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

8.1.4. 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.

8.1.5. Персональные данные могут быть получены Банком от лица, не являющегося субъектом персональных данных (третьего лица).

Если персональные данные получены не от субъекта персональных данных, должностные лица, ответственные за предоставление (осуществление) соответствующей функции, в случаях, предусмотренных Федеральным законом № 152-ФЗ, до начала обработки таких персональных данных обязаны уведомить субъекта персональных данных.

8.1.6. В случае если Банк на основании договора поручает обработку персональных данных другому лицу, существенным условием передачи персональных данных является обязанность обеспечения указанным лицом конфиденциальности персональных данных и сохранения цели обработки персональных данных.

Лицо, осуществляющее обработку персональных данных по поручению Банка, обязано соблюдать принципы и правила обработки персональных данных.

В случае, если Банк поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Банк.

Лицо, осуществляющее обработку персональных данных по поручению Банка, несет ответственность перед Банком.

8.1.7. В случае отказа субъекта персональных данных предоставить свои персональные данные, если предоставление персональных данных является обязательным в соответствии с Федеральным законом № 152, лицо, ответственное за обработку персональных данных, обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональных данных.

8.2. Обработка общедоступных и специальных категорий персональных данных.

8.2.1. Банк как Оператор по обработке персональных данных осуществляет обработку специальных и общедоступных персональных данных. Биометрические персональные данные Банком не обрабатываются.

8.2.2. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни не допускается, за исключением случаев:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных (равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью);
- персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно.

Обработка персональных данных о судимости осуществляться Банком в случаях и в порядке, которые определяются в соответствии с федеральными законами Российской Федерации

Обработка специальных категорий персональных данных прекращается Банком, если устранены причины и достигнуты цели, вследствие которых осуществлялась их обработка, если иное не установлено законодательством Российской Федерации.

8.2.3. Обработка общедоступных персональных данных осуществляется в случае:

- получения Банком общедоступных персональных данных из открытых источников в целях выполнения мер по снижению рисков или в целях выполнения требований законодательства Российской Федерации;
- письменного получения Банком согласия работника о переводе персональных данных работника в категорию общедоступных.

При необходимости размещения в публичных источниках Банком персональных данных работников Банка, отнесенных с письменного согласия субъекта в категорию общедоступных, размещение персональных данных согласуется письменно с субъектом персональных данных, руководителем работника – субъекта персональных данных, работником Управления информационной безопасности. При согласовании указывается:

- перечень размещаемых персональных данных;
- ресурс, где будут размещены общедоступные персональных данных;
- срок, на который будут размещены общедоступные персональные данные;
- порядок удаления общедоступных персональных данных в случае отзыва согласия субъекта персональных данных на размещение его персональных данных.

Размещение общедоступных персональных данных без письменного согласия субъектов персональных данных не допускается.

8.2.4. Обработка персональных данных в целях продвижения услуг Банка на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи осуществляется только при условии наличия предварительного согласия субъекта персональных данных.

Банк немедленно прекращает по требованию субъекта персональных данных обработку его персональных данных в целях продвижения своих услуг на рынке.

8.3. Внесение изменений в обрабатываемые персональные данные осуществляются на основании:

- предоставленного субъектом персональных данных заявления о внесении изменений в произвольной форме;
- на основании организационно – распорядительного документа Банка при изменении персональных данных работников Банка в порядке и сроки, установленные кадровым делопроизводством;
- письменного распоряжения начальника Управления клиентского обслуживания (при выявлении фактов обработки ошибочных персональных данных).

Внесение изменений осуществляется уполномоченным работником Банка. При внесении изменений персональных данных в ИСПДн осуществляется протоколирование действий по изменению.

8.4. Передача персональных данных.

8.4.1. Передача персональных данных, обрабатываемых без средств автоматизации, между структурными подразделениями Банка осуществляется по распоряжению руководителей соответствующих структурных подразделений Банка в целях выполнения возложенных функциональных обязанностей.

Не допускается передача персональных данных работниками Банка, не включенными в перечень лиц, допущенных к обработке персональных данных.

Порядок передачи персональных данных между структурными подразделениями Банка регламентирован во внутренних нормативных документах Банка по обеспечению сохранности конфиденциальной информации.

Учету подлежат как оригиналы документов, содержащих персональные данные, так и созданные на их основе копии. Ответственность за соблюдение порядка передачи персональных данных несет руководитель соответствующего структурного подразделения Банка, осуществляющего передачу персональных данных.

8.4.2. Передача персональных данных третьим лицам осуществляется при наличии согласия субъекта персональных данных или в соответствии с требованиями законодательства Российской Федерации в порядке, регламентированном во внутренних

нормативных документах Банка по обеспечению сохранности конфиденциальной информации.

8.4.3. Трансграничная передача персональных данных.

8.4.3.1. В случае необходимости осуществления трансграничной передачи персональных данных Банк, перед совершением такой передачи, обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав Субъектов персональных данных.

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

- наличия согласия в письменной форме субъекта персональных данных;
- предусмотренных законодательством Российской Федерации, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

8.4.3.1. Трансграничная передача персональных данных осуществляется автоматизированным способом с применением мер по защите персональных данных от несанкционированного доступа (криптографических средств, систем, требующих идентификации и аутентификации).

9. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПОРЯДОК ИХ УНИЧТОЖЕНИЯ ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ОБРАБОТКИ И ПРИ НАСТУПЛЕНИИ ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ

9.1. **Сроки обработки персональных данных.**

Обработка персональных данных прекращается при достижении целей такой обработки, а также по истечении срока, предусмотренного законодательством Российской Федерации, договором, или согласием субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

При отзыве субъектом персональных данных согласия на обработку его персональных данных Обработка осуществляется только в пределах, необходимых для исполнения заключенных с ним договоров и в целях, предусмотренных законодательством Российской Федерации.

9.2. Хранение персональных данных.

9.2.1. При осуществлении хранения персональных данных Банк использует базы данные, находящиеся на территории Российской Федерации, в соответствии с частью 5 статьи 18 Федерального закона № 152-ФЗ.

9.2.2. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом № 152-ФЗ, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

9.2.3. Персональные данные, неиспользуемые в операционной деятельности Банка, и цель обработки которых не достигнута, могут быть переведены на архивное хранение с соблюдением всех необходимых требований, предусмотренных Федеральным законом от 22.10.2001 №125-ФЗ «Об архивном деле в Российской Федерации»", Положением Росархива № 1, Банка России № 801-П от 12.07.2022 «Об утверждении Перечня документов, образующихся в процессе деятельности кредитных организаций, с указанием сроков их

хранения» и иными нормативными актами в сфере организации хранения, комплектования, учета и использования архивных документов.

Архивирование документов, содержащих персональные данные, осуществляется в установленном в Банке порядке. Обязательным условием архивирования персональных данных является обеспечение их конфиденциальности и безопасности.

9.2.4. При хранении персональных данных Банк обеспечивает:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных или на бумажные документы, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

9.3. Порядок уничтожения персональных данных.

9.3.1. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению или обезличиванию в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных или с даты поступления указанного отзыва, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- Банк не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или иными федеральными законами;
- иное не предусмотрено иным соглашением между Банком и субъектом персональных данных.

9.3.2. В случае обращения Субъекта персональных данных к Банку с требованием о прекращении обработки персональных Банк в срок, не превышающий 10 (десяти) рабочих дней с даты получения соответствующего требования, прекращает их обработку или обеспечивает прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона № 152-ФЗ. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления Банком в адрес Субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

9.3.3. В целях уничтожения обработанных персональных данных приказом Председателя Правления Банка создается комиссия.

Уничтожение обработанных персональных данных производится комиссией с составлением соответствующего акта (образец акта указан в Приложении № 2 к Политике), который утверждается Председателем Правления Банка или лицом, его замещающим.

9.3.4. Способы уничтожения персональных данных:

Вид носителя персональных данных	**Способ уничтожения**
Жесткий диск	1.Многократная перезапись данных 2.Стирание с помощью программных средств уничтожения информации 2. Разбор носителя и физическое его уничтожение
Гибкий магнитный диск	1.Многократная перезапись данных

	2. Разбор носителя и физическое его уничтожение в шредере с последующей термической обработкой (сжиганием)
Флеш-носитель	1. Многократная перезапись данных 2. Термическая обработка (сжигание)
CD и DVD-диски	1. Многократная перезапись данных (если применима) 2. Термическая обработка (сжигание)
Бумажный носитель	1. Уничтожение носителя в шредере 2. Сжигание

9.3.5. Хранение Актов уничтожения персональных данных осуществляется в течение срока исковой давности, если иное не установлено законодательством Российской Федерации.

9.3.6. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных в ч.3-5.1 ст.21 Федерального закона №152-ФЗ, 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 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

9. УСТРАНЕНИЕ НАРУШЕНИЙ, ДОПУЩЕННЫХ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. В случае выявления недостоверных персональных данных или неправомерных действий с ними Банка при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных, Банк обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

10.2. В случае подтверждения факта недостоверности персональных данных Банк на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

10.3. В случае выявления неправомерных действий с персональными данными Банк в срок, не превышающий 3 (трех) рабочих дней с даты такого выявления, обязан прекратить неправомерную обработку персональных данных. устранить допущенные нарушения.

В случае если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение.

Об устранении допущенных нарушений или об уничтожении персональных данных Банк уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных - также указанный орган.

10.3.1. 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 24 (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 72 (семидесяти двух) часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

10.4. Выявленные нарушения при обработке персональных данных фиксируются на основании оформления инцидента информационной безопасности.

10.5. Работником Банка, ответственным за устранение выявленных нарушений, является работник, назначенный организационно – распорядительным документом лицом, ответственным за информационную безопасность персональных данных.

10.6. Работником, ответственным за контроль устранения выявленных нарушений, является работник, назначенный ответственным лицом за организацию обработки персональных данных.

10. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИИ

11.1. Порядок предоставления информации по запросу Уполномоченного органа по защите прав субъектов персональных данных.

11.1.1. Поступивший от уполномоченного органа запрос регистрируется в Банке в соответствии с порядком, установленным документооборотом Банка.

11.1.2. После регистрации запрос направляется на рассмотрение:

- работнику Банка, назначенному Ответственным за организацию обработки персональных данных;
- работнику Юридического управления.

11.1.3. Ответственное лицо за организацию обработки персональных данных подготавливает ответ на запрос в течение 10 (десяти) рабочих дней с даты получения такого запроса, согласовывает ответ с Юридическим управлением, Управлением клиентского обслуживания (если запрос относится к персональным данным клиента Банка), Секретариатом (если запрос относится к персональным данным работника Банка), работником службы внутреннего контроля, иными работниками Банка (в соответствии с резолюцией руководства Банка).

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

11.1.4. Ответственное лицо за организацию обработки персональных данных при подготовке ответа на запрос уполномоченного органа обязан руководствоваться требованиями законодательства Российской Федерации в области обработки персональных данных.

11.1.5. Подготовленный, согласованный и подписанный руководством Банка ответ на запрос направляется уполномоченному органу.

11.2. Порядок предоставления информации по запросу субъекта персональных данных.

11.1.1. Банк обязан сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу последнего в течение 10 (десяти) рабочих дней с момента обращения либо получения запроса. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления Банком в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Запрос предоставляется в произвольной письменной форме и должен содержать сведения, указанные в части 3 статьи 14 Федерального закона № 152-ФЗ.

Банк предоставляет сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

11.1.2. Субъект персональных данных вправе обратиться повторно в Банк или направить повторный запрос в целях получения сведений, предусмотренных частью 7 статьи 14 Федерального закона № 152-ФЗ, а также в целях ознакомления с обрабатываемыми персональными данными 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 должен содержать обоснование его повторного направления.

11.1.3. Сведения об обращениях субъекта персональных данных фиксируются в Журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных по форме Приложения № 3 к Политике).

11.1.4. Обработку обращений субъектов персональных данных осуществляет работник Банка, назначенный Ответственным лицом за организацию обработки персональных данных.

11.1.5. Ответственное лицо за организацию обработки персональных данных рассматривает возможность предоставления субъекту персональных данных информации о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, о возможности ознакомления с ними на основании законодательства Российской Федерации, в том числе положениями Федерального закона № 152-ФЗ.

11.1.6. По результатам рассмотрения обращения в течение 10 рабочих дней Ответственное лицо за организацию обработки персональных данных:

- сообщает субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с персональными данными;
- либо выносит мотивированный отказ. В случае отказа в предоставлении сведений о наличии персональных данных в срок, не превышающий 10 рабочих дней с даты получения запроса субъекта персональных данных или со дня обращения субъекта персональных данных, дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона Российской Федерации, являющееся основанием для такого отказа.

11.1.7. Возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, предоставляется субъекту персональных данных (его представителю) безвозмездно.

11.1.8. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных:

- сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, - Банк обязан внести в них необходимые изменения;
- сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, - Банк обязан уничтожить такие персональные данные.

11.1.9. О внесенных изменениях и предпринятых мерах Банк уведомляет субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

11.3. Порядок предоставления информации по запросу правомочных лиц.

В случае если запрошенные акционером и лицами, реализующим права по акциям, а также их представителям (далее – правомочные лица) документы Банка содержат персональные данные и отсутствует согласие субъекта персональных данных на их предоставление третьим лицам, Банк обязан предоставить правомочному лицу запрошенные

документы Банка, скрыв в них соответствующие персональные данные за исключением фамилии, имени и отчества субъекта персональных данных.

12. РЕАЛИЗУЕМЫЕ БАНКОМ ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Банк принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

12.2. Состав указанных в пункте 12.1. Политики мер, включая их содержание и выбор средств защиты персональных данных, определяется во внутренних нормативных документах Банка исходя из требований:

- Федерального закона № 152-ФЗ;
- главы 14 Трудового кодекса Российской Федерации;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- иных нормативных правовых актов Российской Федерации об обработке и защите персональных данных.

12.3. В предусмотренных законодательством случаях обработка персональных данных осуществляется Банком с согласия Субъектов персональных данных.

Банком производится устранение выявленных нарушений законодательства Российской Федерации об обработке и защите персональных данных.

12.4. Хранение персональных данных осуществляется в форме, позволяющей определить Субъекта персональных данных, не дольше чем этого требуют цели обработки персональных данных, если срок хранения не установлен Федеральным законом № 152-ФЗ, договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных.

12.5. Банком осуществляется ознакомление Работников Банка, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, Политикой и иными внутренними нормативными документами Банка по вопросам обработки персональных данных, и (или) обучение указанных Работников Банка по вопросам обработки и защиты персональных данных.

12.6. При обработке персональных данных с использованием средств автоматизации Банком, в частности, применяются следующие меры:

1) назначается Ответственный за организацию обработки персональных данных;

2) утверждаются (издаются) внутренние нормативные документы Банка по вопросам обработки и защиты персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей

их обработки или при наступлений иных законных оснований, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ;

4) осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Политике и внутренним нормативным документам Банка;

5) проводится оценка вреда, который может быть причинен Субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, определяется соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение исполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

6) ознакомление 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, внутренними нормативными документами Банка по вопросам обработки персональных данных, и (или) обучение указанных работников.

12.7. Обеспечение безопасности персональных данных в Банке при их обработке в ИСПДн достигается путем:

1) определения угроз безопасности персональных данных при их обработке в ИСПДн. Тип актуальных угроз безопасности персональных данных и необходимый уровень защищенности персональных данных определяются в соответствии с требованиями законодательства Российской Федерации и с учетом проведения оценки возможного вреда;

2) применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, обеспечивающих определенные уровни защищенности персональных данных, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.

3) применения прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

4) оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

5) учета машинных носителей персональных данных;

6) обнаружения фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них;

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

8) установления правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;

9) контроля за принимаемыми мерами по обеспечению безопасности персональных данных, уровня защищенности ИСПДн.

12.8. Обеспечение защиты персональных данных в Банке при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

1) обособления персональных данных от иной информации;

2) недопущения фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;

3) использования отдельных материальных носителей для обработки каждой категории персональных данных;

4) принятия мер по обеспечению раздельной обработки персональных данных 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;

5) соблюдения требований:

- к раздельной обработке зафиксированных на одном материальном носителе персональных данных и информации, не относящейся к персональным данным;
- уточнению персональных данных;
- уничтожению или обезличиванию части персональных данных;
- использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них персональных данных;
- ведению журналов, содержащих персональные данные, необходимых для выдачи однократных пропусков Субъектам персональных данных в занимаемые Банком здания и помещения;
- хранению персональных данных, в том числе к обеспечению раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

13. ДОСТУП К ОБРАБАТЫВАЕМЫМ БАНКОМ ПЕРСОНАЛЬНЫМ ДАННЫМ

13.1. Доступ к обрабатываемым в Банке персональным данным имеют работники Банка, уполномоченные организационно-распорядительным документом Банка, лица, которым Банк поручило обработку персональных данных на основании заключенного договора, а также лица, чьи персональные данные подлежат обработке.

13.2. В целях разграничения доступа к обработке персональных данных организационно – распорядительным документом Банка устанавливается перечень структурных подразделений и работников Банка, допущенных к обработке персональных данных, с указанием персональных данных, доступ к которым разрешен в целях выполнения функциональных обязанностей.

13.3. Доступ Работников Банка к обрабатываемым персональным данным осуществляется в соответствии с их должностными обязанностями и требованиями внутренних нормативных документов Банка.

Допущенные к обработке персональных данных Работники Банка под роспись знакомятся с внутренними нормативными документами Банка, устанавливающими порядок обработки персональных данных, включая документы, устанавливающие права и обязанности конкретных Работников Банка.

13.4. Порядок доступа Субъекта персональных данных к его персональным данным, обрабатываемым Банком, определяется в соответствии с законодательством Российской Федерации и внутренними нормативными документами Банка.

14. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

14.1. Персональные данные относятся к сведениям конфиденциального характера и охраняются в соответствии с внутренним нормативным документом Банка по защите сведений конфиденциального характера.

14.2. Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания;

- в других случаях, предусмотренных законодательством Российской Федерации.

14.3. Работники Банка, имеющие доступ к персональным данным, в том числе осуществляющие их обработку, обязаны хранить банковскую и коммерческую тайну в соответствии с законодательством Российской Федерации и внутренними документами Банка, а также:

- не разглашать персональные данные третьим лицам, не имеющим в установленном порядке права доступа к персональным данным, обрабатываемым в Банке;
- не передавать и не раскрывать третьим лицам сведения о персональных данных;
- в случае попытки третьих лиц получить конфиденциальные сведения немедленно сообщить об инциденте уполномоченному работнику Банка;
- не использовать сведения о персональных данных с целью получения выгоды.

15. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Работники Банка, имеющие доступ к персональным данным и виновные в нарушении требований законодательства Российской Федерации, Политики и внутренних нормативных документов Банка, регулирующих обработку, защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

16. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

16.1. Политика подлежит размещению на официальном сайте Банка в сети Интернет.

16.2. Политика применяется совместно с другими внутренними нормативными документами Банка, регулирующими обработку, защиту персональных данных и защиту информационной безопасности.

16.3. Вопросы, не урегулированные в Политике, решаются в соответствии с законодательством Российской Федерации, нормативными актами Банка России, регулирующими обработку, защиту персональных данных и защиту информационной безопасности.

16.4. Политика вступает в действие с момента его утверждения уполномоченным органом управления Банка либо с даты, указанной в соответствующем решении органа управления Банка.

16.5. В случае, если при изменении законодательства Российской Федерации отдельные пункты Политики вступают в противоречия с данными изменениями, то эти пункты утрачивают силу и до момента внесения соответствующих изменений в Политику Работники Банка руководствуются законодательством Российской Федерации.

16.7. Контроль исполнения требований Политики осуществляется Ответственным лицом за организацию обработки персональных данных в Банке.

Приложение 1
к Политике в отношении обработки
персональных данных в АО КБ «КОСМОС»

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Москва «__» _____20__ г.

Я,_____,
(Фамилия, Имя, Отчество полностью)

_____ _____серия_____№_____, выдан____ _____
(вид документа, удостоверяющего личность)

_____
(кем и когда)

зарегистрированный(ая) по адресу:_____
_____

в соответствии со статьей 9 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» даю свое согласие Акционерному обществу Коммерческому банку «КОСМОС», расположенному по адресу: 123317, г. Москва, Красногвардейский бульвар, д. 7, стр. 1 (далее - Банк), на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 статьи 3 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (включая получение от меня и/или от любых третьих лиц).

1. Под персональными данными понимается любая информация, относящаяся к моей личности, в том числе: мои фамилия, имя, отчество, год, месяц, число и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и любая иная информация, относящаяся, доступная, либо известная Банку в результате нашего сотрудничества в соответствии с заключенными договорами (далее – «Персональные данные»).

2. Под обработкой моих Персональных данных понимается: сбор, систематизация, составление перечней, маркировка, накопление, запись на электронные носители, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение, трансграничная передача Персональных данных, как с использованием средств автоматизации, так и без их использования, а также осуществление иных действий с моими Персональными данными в соответствии с законодательством Российской Федерации при условии соблюдения Банком конфиденциальности моих Персональных данных.

3. Мои персональные данные могут быть раскрыты Банком в необходимом объеме третьим лицам при наличии законного основания при заключении, изменении, исполнении или расторжении договоров между мной и Банком, а также при необходимости привлечения Банком третьих лиц к оказанию услуг по совершению указанных в пункте 2 настоящего Согласия действий с Персональными данными и/или передаче Банком принадлежащих ему функций и полномочий в сфере обработки Персональных данных третьим лицам.

4. Настоящее Согласие вступает в силу с момента его подписания и действует до дня отзыва в письменной форме.

5. После прекращения сотрудничества между мной и Банком, предусмотренного договорами, мои Персональные данные могут находиться на хранении в Банке в архивированном виде в пределах сроков хранения документов, предусмотренных законодательством об архивном деле в Российской Федерации.

_____ (_____) «____»_____20__г.

Приложение 2
к Политике в отношении обработки
персональных данных в АО КБ «КОСМОС»
УТВЕРЖДАЮ
Председатель Правления
АО КБ «КОСМОС»
_____(_____)

«___»_____20____г.

Акт об уничтожении персональных данных[1]
№ ____ от «___»_____ 20__года

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела аудит в АО КБ «КОСМОС» персональных данных (далее – ПДн) и установила, что, в соответствии с требованиями нормативных документов по обработке ПДн, информация подлежит уничтожению:

N п/п	Регистрационный номер носителя ПДн	Наименование АБС/документа, содержащих уничтожаемые ПДн	Категории ПДн, подлежащие уничтожению	Основание для уничтожения	Кол-во записей для уничтожения

Всего подлежит уничтожению _____(_____) записей
(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации, сжигания и т.п.)

N п/п	Регистрационный номер носителя ПДн	Наименование АБС/документа, содержащих уничтожаемые ПДн	Кол-во записей, содержащих ПДн, до уничтожения[2]	Кол-во записей, содержащих ПДн, после уничтожения	Подпись лица, производив. удаление ПДн

Председатель комиссии: _____ / /
Члены комиссии: _____ / /
_____ / /

Настоящий Акт составлен в единственном экземпляре, хранящемся в:
_____.

[1] Примечания:
1. Акт составляется раздельно на каждый способ уничтожения носителей.
2. Все листы акта, а также все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

[2] Примечания:
В расчет включаются записи в указанной АБС, содержащие ПДн, владелец которых может быть прямо или косвенно установлен.

Приложение 3
к Политике в отношении обработки
персональных данных в АО КБ «КОСМОС»

Журнал учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных в АО КБ «КОСМОС»

Журнал начат "__" _____ 20_ г. Журнал завершен "__" _____ 20_ г.

_____ /ФИО должностного лица/ _____ /ФИО должностного лица/

На _____ листах

N п/п	Сведения о запрашивающем субъекте ПДн	Краткое содержание обращения	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении	Номер и дата документа о передаче информации/ об отказе в предоставлении информации	Подпись ответственного лица за предоставление информации	Примечание
1	2	3	4	5	6	7	8