

БАЙКАЛКРЕДОБАНК

КОММЕРЧЕСКИЙ БАНК



УТВЕРЖДЕНО

Правлением КБ «Байкалкредобанк» (ПАО)

Протокол № 100 от «11» 12 2018 г.

Председатель Правления

Ген / А.Н. Геряев



**ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
КБ «Байкалкредобанк» (ПАО)**

Раздел I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке и защите персональных данных КБ «Байкалкредобанк» (ПАО) (далее – Положение) устанавливает порядок обработки персональных данных Работников, Контрагентов, Клиентов, их представителей, иных лиц в КБ «Байкалкредобанк» (ПАО) (далее Банк, или Работодатель, или Оператор) и гарантии конфиденциальности сведений, предоставляемых указанными лицами Банку.

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иными нормативными актами, действующими на территории Российской Федерации.

1.3. В настоящем Положении используются следующие термины и определения:

- **Работник** - физическое лицо (субъект персональных данных), заключившее с Банком (Работодателем) трудовой договор.

- **Субъект персональных данных** – физическое лицо, являющееся Работником Банка, Контрагентом, Клиентом Банка (Частный Клиент), либо представляющее интересы клиента Банка – юридического лица (представитель Корпоративного Клиента).

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

- **Контрагент** – физическое лицо, вступившее в договорные отношения с Банком.

- **клиент** – Частный Клиент и/или Корпоративный Клиент Банка.

- **Частный Клиент Банка** - физическое лицо, заключившее с Банком письменный договор на оказание банковских и иных услуг, а также его представитель на основании закона или доверенности.

- **Корпоративный Клиент Банка** - юридическое лицо, которому Банк оказывает услуги в рамках имеющейся у него лицензии Банка России на основании соответствующего договора.

- **Представитель Корпоративного Клиента** – лицо:

• входящее в состав органов управления Корпоративного Клиента (включая, но не ограничиваясь следующей номенклатурой должностей: генеральный директор, заместитель генерального директора, исполнительный директор, председатель правления, член правления, председатель совета директоров, член совета директоров, председатель наблюдательного совета, член наблюдательного совета, управляющий, конкурсный управляющий),

• являющееся владельцем/учредителем/акционером/участником Корпоративного Клиента,

• действующее от имени Корпоративного Клиента на основании доверенности,

• указанное в карточке с образцами подписей и оттиска печати (альбоме образцов подписей лиц, уполномоченных распоряжаться денежными средствами, находящимися на банковском счете) Корпоративного Клиента.

- **Официальный представитель** – физическое лицо, уполномоченное на представление в Банке интересов юридического лица, индивидуального предпринимателя, физического лица, вступившее в договорные отношения с Банком.

- **Персональные данные (ПДн)** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), необходимая Оператору в связи с исполнением договорных и иных отношений, и касающаяся конкретного Работника, Контрагента, Клиента, их представителей, иных лиц, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия (должность), номер контактного телефона, адрес электронной почты, данные паспорта, удостоверяющего его личность, сведения о дате его выдачи и выдавшем его органе, реквизиты доверенности, подтверждающей полномочия представителя Работника, Контрагента, Клиента, иных лиц, сведения об ИНН, СНИЛСе.

- **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.

- **Биометрические персональные данные** - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных.

- **Защита персональных данных** – деятельность Банка по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер обеспечения конфиденциальности информации.

- **Конфиденциальность персональных данных** – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения и передачи третьим лицам без согласия субъекта персональных данных или наличия иного законного основания.

- **Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

- **Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

- **Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

- **Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

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

- **ИСПДн** – информационная система персональных данных, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

- **Автоматизированная обработка ПДн** – обработка ПДн с помощью средств вычислительной техники.

- **Обработка ПДн без использования средств автоматизации** - обработка персональных данных, содержащихся в информационной системе персональных данных, либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

- **Актуальные угрозы безопасности персональных данных** - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

- Система защиты персональных данных (СЗПДн) - организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

1.4. Настоящее Положение (изменения к нему) утверждается Правлением Банка и действует до его отмены распорядительным документом Банка или до его замены иным аналогичным внутренним документом Банка. Все Работники Банка должны быть ознакомлены под роспись с данным Положением (изменениями к нему).

1.5. Настоящее Положение является обязательным для исполнения всеми Работниками Банка, имеющими доступ в Банке к персональным данным Работников, Контрагентов, Клиентов, их представителей, иных лиц.

1.6. Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм Положения возлагается на назначаемого приказом по Банку уполномоченного сотрудника, ответственного за обеспечение безопасности информационных систем персональных данных.

Раздел I. ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ

1. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ ЧАСТНЫХ КЛИЕНТОВ

1.1. Состав персональных данных Частного Клиента, обработка которых осуществляется Банком:

- фамилия, имя, отчество;
- паспортные данные, включая серию и номер паспорта, сведения о дате выдачи и выдавшем паспорт органе; дата рождения, место рождения, пол, адрес регистрации;
- данные паспорта или иного документа, удостоверяющего личность иностранного гражданина, включая номер, сведения о дате выдачи и выдавшем органе, срок действия; дата рождения, пол;
- данные миграционных документов Частного Клиента – иностранного гражданина или лица без гражданства: визы, миграционной карты, уведомления Федеральной миграционной службы о месте пребывания;
- гражданство;
- адрес регистрации иностранного гражданина в стране, гражданином которой он/она является;
- адрес местонахождения (места пребывания) Частного Клиента;
- контактная информация, включая номера телефонов, факсов, e-mail;
- занимаемая(ые) должность(и) Частного Клиента;
- сведения о трудовой деятельности;
- семейное положение;
- состав семьи;
- данные свидетельства о рождении ребенка;
- данные свидетельства о заключении брака;
- социальное положение;
- имущественное положение;
- сведения о доходах Частного Клиента и их источниках;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства;
- номер счёта в иных кредитных организациях;
- иные сведения.

1.2. Указанные в пункте 1.1. персональные данные обрабатываются в целях исполнения обязательств Банка по договорам с Частными Клиентами, а также на основании и во исполнение:

- Федерального закона «О банках и банковской деятельности»,
- Федерального закона «О противодействии легализации доходов, полученных преступным путём, финансированию терроризма»
- иных законов и подзаконных актов, регулирующих деятельность Банка.

1.3. Обработка персональных данных Частного Клиента производится с его письменного согласия, оформленного (в зависимости от вида заключаемого с Банком договора) в соответствии с Приложениями № 3 или 4 к настоящему Положению.

2. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРЕДСТАВИТЕЛЕЙ КОРПОРАТИВНЫХ КЛИЕНТОВ

2.1. В отношении представителей Корпоративных Клиентов Банк осуществляет обработку следующих персональных данных:

- фамилия, имя, отчество;
- паспортные данные, включая номер паспорта, сведения о дате выдачи и выдавшем паспорт органе, дату рождения, место рождения, пол, адрес регистрации;

- данные паспорта или иного документа, удостоверяющего личность иностранного гражданина, включая номер, сведения о дате выдачи и выдавшем органе, срок действия, дату рождения, пол;

- данные миграционных документов иностранного гражданина или лица без гражданства: визы, миграционной карты, уведомления Федеральной миграционной службы о месте пребывания;

- адрес регистрации иностранного гражданина в стране, гражданином которой он/она является;

- адрес местонахождения (места пребывания);

- занимаемая(ые) должность(и).

2.2. Указанные в пункте 2.1 настоящего раздела персональные данные обрабатываются в целях исполнения Федерального закона "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".

2.3. В связи с тем, что обработка персональных данных, указанных в п. 2.1 настоящего раздела, осуществляется в соответствии с Федеральным законом "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма", устанавливающим цель обработки, условия получения персональных данных, круг субъектов, персональные данные которых подлежат обработке, полномочия оператора, получение согласий на обработку персональных данных в данном случае не требуется.

3. СОСТАВ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ

3.1. Состав биометрических персональных данных Частного Клиента, обработка которых осуществляется Банком:

- изображение лица, полученное с помощью фото- и видеоустройств;
- голос, полученный с помощью звукозаписывающих устройств.

4. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Сведения, перечисленные в статьях 1, 2, 3 настоящего раздела, являются конфиденциальными. Банк обеспечивает конфиденциальность персональных данных, и обязан не допускать их распространения без согласия клиентов, либо наличия иного законного основания.

4.2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных клиентов распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

4.3. Режим конфиденциальности персональных данных снимается в случаях обезличивания или опубликования их в общедоступных источниках (СМИ, Интернет, ЕГРЮЛ и иных публичных государственных реестрах).

5. ПРАВА И ОБЯЗАННОСТИ БАНКА КАК ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обработка персональных данных Частных Клиентов и представителей Корпоративных Клиентов осуществляется Банком с письменного согласия субъектов персональных данных, за исключением случаев, предусмотренных пунктом 5.2 настоящего раздела. Обязанность представить доказательство получения согласия на обработку персональных данных клиентов возлагается на Банк.

5.2. Банк имеет право без согласия субъекта персональных данных осуществлять обработку его персональных данных в следующих случаях:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

5.3. Обработка биометрических персональных данных Частных Клиентов и представителей Корпоративных Клиентов осуществляется Банком с письменного согласия субъектов персональных данных, за исключением случаев, предусмотренных пунктом 5.4 настоящего раздела. Обязанность представить доказательство получения согласия на обработку персональных данных возлагается на Банк.

5.4. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

5.5. В целях обеспечения прав и свобод человека и гражданина Банк и его работники при обработке персональных данных клиента обязаны соблюдать следующие общие требования.

5.5.1. При определении объема и содержания персональных данных клиента, подлежащих обработке, Банк должен руководствоваться Федеральным законом «О персональных данных», законодательством, регулирующим деятельность Банка, договорными обязательствами, принятыми на себя сторонами по договору между клиентом и Банком. Банк получает персональные данные клиента только в объеме, необходимом для достижения целей надлежащего исполнения договора с клиентом и соблюдения применимого к Банку законодательства.

5.5.2. Банк не должен обрабатывать не являющиеся общедоступными персональные данные Частного Клиента или представителя Корпоративного Клиента о его судимости, политических, религиозных и иных убеждениях и частной жизни.

5.5.3. Банк не должен запрашивать информацию о состоянии здоровья Частного Клиента или представителя Корпоративного Клиента.

5.6. Банк должен за собственный счет обеспечить защиту персональных данных Частного Клиента, представителя Корпоративного Клиента от неправомерного их использования или утраты в порядке, установленном федеральным законодательством.

5.7. В случае, если Банк на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

5.8. Банк может осуществлять трансграничную передачу персональных данных на территории иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

5.8.1. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случае наличия согласия в письменной форме субъекта персональных данных.

6. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у Банка персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими

персональными данными. Субъект персональных данных вправе требовать от Банка уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных Банком в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

6.3. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю Банком при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

6.4. Субъект персональных данных имеет право на получение при обращении или при направлении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных Банком, а также цель такой обработки;
- 2) способы обработки персональных данных, применяемые Банком;
- 3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- 4) перечень обрабатываемых персональных данных и источник их получения;
- 5) сроки обработки персональных данных, в том числе сроки их хранения;
- 6) сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

6.5. Субъект персональных данных имеет право отозвать согласие на обработку персональных данных, ограничить способы и формы обработки персональных данных, запретить распространение персональных данных без его согласия.

6.6. Субъект персональных данных вправе обжаловать действия или бездействие Банка в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

7. ПОРЯДОК ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ БАНКОМ

7.1. Банк получает персональные данные Частного Клиента:

- непосредственно от субъекта персональных данных – Частного Клиента, в связи с заключением с Частным Клиентом письменного договора и/или подписания заявления на открытие банковского счёта, содержащих письменное согласие на обработку персональных данных.

- от законного представителя Частного Клиента (субъекта персональных данных).

Если персональные данные Частного Клиента получены Банком от третьего лица, Банк до начала обработки этих персональных данных предоставляет Частному Клиенту письменную информацию о своём наименовании и адресе, правовом основании и цели обработки Банком персональных данных Частного Клиента, о предполагаемых пользователях персональных данных и установленных Федеральным законом «О персональных данных» правах Частного Клиента.

- из общедоступных источников персональных данных, включая СМИ и Интернет.

7.2. Банк получает персональные данные представителя Корпоративного Клиента:

- от представителя Корпоративного Клиента (субъекта персональных данных);
- от иных представителей Корпоративного Клиента – только на основании федерального закона или только общедоступные персональные данные.

• из общедоступных источников персональных данных, включая СМИ, Интернет, ЕГРЮЛ и иные публичные государственные реестры.

8. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Обработка персональных данных, указанных в статьях 1 и 2 настоящего раздела, осуществляется Банком исключительно для достижения целей, определенных письменным договором между Частным/Корпоративным Клиентом и Банком, и исполнения действующего законодательства.

8.2. Обработка Банком персональных данных, указанных в статьях 1 и 2 настоящего раздела, заключается в получении, систематизации, накоплении, хранении, уточнении (обновлении, изменении), использовании, распространении, обезличивании, блокировании, уничтожении и в защите от несанкционированного доступа.

8.3. Обработка персональных данных, указанных в статьях 1 и 2 настоящего раздела, ведется методом смешанной (в том числе автоматизированной) обработки.

8.4. К обработке персональных данных Клиента могут иметь доступ только работники Банка, допущенные к работе с досье Частных Клиентов и Корпоративных Клиентов, а также занимающиеся обработкой (платёжных) поручений указанных клиентов.

8.5. В случае соответствующего обращения субъекта персональных данных, Банк обязан произвести необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Банк, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Банк обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

8.6. Банк уничтожает персональные данные Частного Клиента или представителей Корпоративного Клиента в следующие сроки:

- в течение трёх рабочих дней со дня выявления неправомерных действий с персональными данными;

- хранящиеся на электронных носителях - в течение трех рабочих дней со дня окончания срока хранения, установленного законом, срока исковой давности по договору с клиентом;

- хранящиеся на бумажных носителях и не отнесенные к разряду первичных бухгалтерских документов или иных документов, подлежащих хранению по законодательству Российской Федерации - в течение трех рабочих дней со дня окончания срока исковой давности по договору с клиентом;

- хранящиеся на бумажных носителях и отнесенные к разряду первичных бухгалтерских документов либо документов, подлежащих хранению по законодательству Российской Федерации, в течение трех рабочих дней со дня окончания срока их хранения, установленного нормами законодательства Российской Федерации.

8.7. Персональные данные, в том числе биометрические, не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено в соответствии с законодательством.

9. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Передача персональных данных, указанных в статьях 1 и 2 настоящего раздела, осуществляется Банком исключительно для достижения целей, определенных письменными договорами между клиентом и Банком.

9.2. Передача персональных данных, указанных в статьях 1 и 2 настоящего раздела, третьим лицам осуществляется Банком только на основании соответствующего договора, существенным

условием которого является обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Данное положение не распространяется на случаи обезличивания персональных данных и в отношении общедоступных персональных данных.

9.3. Передача персональных данных третьим лицам осуществляется с использованием внутренней сети, по каналам связи с использованием необходимых средств защиты и на бумажных носителях.

9.4. Банк осуществляет трансграничную передачу персональных данных, указанных в статьях 1 и 2 настоящего раздела, в том числе на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, только в целях исполнения договора с клиентом, при наличии соответствующего письменного согласия субъекта персональных данных.

9.5. Передача персональных данных государственным органам осуществляется в рамках их полномочий в соответствии с применимым законодательством.

10. ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Персональные данные, указанные в статьях 1 и 2 настоящего раздела, могут храниться, как на бумажных носителях, так и в электронном виде.

10.2. Персональные данные, указанные в статьях 1 и 2 настоящего раздела, могут вноситься Банком или клиентами в следующие группы документов:

- письменные договоры с клиентами;
- расчётные (платёжные) документы клиентов;
- заявления, распоряжения, иные письменные поручения клиентов;
- письменные претензии клиентов по качеству предоставленных услуг;
- письменные документы (судебные иски, возражения на иски, решения судебных инстанций и т.п.), связанные с ведением судебного делопроизводства по искам клиентов против Банка или Банка против клиента;
- корреспонденцию с клиентами по прочим вопросам.

10.3. Персональные данные на бумажных носителях, если с них не снят на законном основании режим конфиденциальности, хранятся в специально отведенных шкафах, запирающихся на ключ.

10.3.1. Ключи от железных шкафов хранятся лично у работников Банка, допущенных к обработке персональных данных Частных Клиентов, представителей Корпоративных Клиентов и/или у руководителя соответствующего подразделения Банка.

10.4. Персональные данные, указанные в статьях 1 и 2 настоящего раздела, также хранятся в электронном виде: во внутренней сети Банка, с доступом для работников, допущенных к обработке персональных данных Частных Клиентов, представителей Корпоративных Клиентов.

11. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ КЛИЕНТА

11.1. Право доступа к персональным данным Частных Клиентов и/или представителей Корпоративных Клиентов Банка имеют:

- Председатель Правления Банка, члены Правления;
- работники Банка, осуществляющие непосредственную работу с Частными Клиентами и/или представителями Корпоративных Клиентов Банка;
- работники операционных подразделений Банка, в объеме, необходимом для исполнения их трудовых обязанностей;
- работники, осуществляющие в Банке бухгалтерский учёт и участвующие в подготовке отчётности, согласно требованиям действующего законодательства, в объеме, необходимом для исполнения их трудовых обязанностей;
- работники подразделений, осуществляющих внутренний контроль в Банке, в объеме, необходимом для исполнения их трудовых обязанностей;
- другие сотрудники Банка при условии оформления в произвольной форме временного допуска к персональным данным клиента Банка за подписью руководителя подразделения Банка,

в котором работает данный сотрудник, сотрудника по информационной безопасности, и Председателя Правления Банка

11.2. Доступ субъекта персональных данных к своим персональным данным предоставляется при личном обращении в Банк либо при получении Банком письменного запроса. Банк обязан сообщить субъекту персональных данных информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение десяти рабочих дней с момента обращения.

11.3. При передаче персональных данных Банк должен соблюдать следующие требования:

- не сообщать персональные данные, указанные в статьях 1 и 2 настоящего раздела, третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, установленных федеральным законом;

- не сообщать персональные данные, указанные в статьях 1 и 2 настоящего раздела, в коммерческих целях без письменного согласия субъекта персональных данных;

- предупредить лиц, получающих персональные данные, указанные в статьях 1 и 2 настоящего раздела, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

- разрешать доступ к персональным данным, указанным в статьях 1 и 2 настоящего раздела, только специально уполномоченным лицам; эти лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

12. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ЧАСТНЫХ КЛИЕНТОВ И ПРЕДСТАВИТЕЛЕЙ КОРПОРАТИВНЫХ КЛИЕНТОВ

12.1. Защите подлежит следующая информация о клиентах, если с неё на законном основании не снят режим конфиденциальности:

- документы, содержащие персональные данные Частного Клиента или представителей Корпоративного Клиента;

- информация, содержащая персональные данные Частного Клиента или представителей Корпоративного Клиента, размещенная на электронных носителях.

12.2. Банк обязан при обработке персональных данных Частных Клиентов и представителей Корпоративных Клиентов принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

12.3. Общую организацию защиты персональных данных Частных Клиентов и представителей Корпоративных Клиентов осуществляют руководители соответствующих подразделений, в которых осуществляется их обработка.

12.4. Защита персональных данных Частных Клиентов и представителей Корпоративных Клиентов, хранящихся в электронных базах данных Банка, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается работниками Отдела автоматизации и информационного сопровождения при координации специалиста по информационной безопасности.

12.5. Доступ к персональным данным Частных Клиентов и представителей Корпоративных Клиентов имеют сотрудники Банка, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей.

12.6. Сотрудник Банка, имеющий доступ к персональным данным Частных Клиентов или представителей Корпоративных Клиентов в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные Частных Клиентов или представителей Корпоративных Клиентов, исключающее доступ к ним третьих лиц;

- в отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные Частных Клиентов или представителей Корпоративных Клиентов;

- на период отпуска, во время служебной командировки и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные Частных Клиентов или представителей Корпоративных Клиентов лицу, на которое локальным актом Банка (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, указанные выше

документы и иные носители передаются другому сотруднику, имеющему доступ к персональным данным Частных Клиентов и представителей Корпоративных Клиентов.

12.6.1. При увольнении сотрудника, имеющего доступ к персональным данным Частных Клиентов или представителей Корпоративных Клиентов, документы и иные носители, содержащие персональные данные Клиентов, передаются другому сотруднику, имеющему доступ к персональным данным Частных Клиентов или представителей Корпоративных Клиентов.

12.7. Допуск к персональным данным Частных Клиентов или представителей Корпоративных Клиентов других сотрудников Банка, не имеющих надлежащим образом оформленного доступа, запрещается.

12.8. Документы, содержащие персональные данные Частных Клиентов или представителей Корпоративных Клиентов, хранятся в запирающихся шкафах, обеспечивающих защиту от несанкционированного доступа.

В конце рабочего дня все документы, содержащие персональные данные Клиентов, помещаются в шкафы, обеспечивающие защиту от несанкционированного доступа.

12.9. Защита доступа к электронным базам данных, содержащим персональные данные Клиентов, обеспечивается:

- использованием лицензированных антивирусных и иных программно-технических средств защиты периметра внутренней сети, не допускающих несанкционированный вход в локальную сеть Банка;

- разграничением прав доступа с использованием учетной записи;

- двух ступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных.

12.10. Попытки несанкционированного входа в учётные записи (тремякратный ввод неверного имени пользователя и/или пароля), в которых содержатся персональные данные, приводят к блокировке таких учётных записей.

12.11. Все электронные приложения, содержащие персональные данные, включая информационные системы персональных данных, папки и файлы, содержащие персональные данные, защищаются паролем.

12.12. Копировать и делать выписки персональных данных Частных Клиентов или представителей Корпоративных Клиентов разрешается исключительно в служебных целях с письменного разрешения руководителя соответствующего подразделения Банка, осуществляющего работу с клиентами.

В случае если копирование или выписка персональных данных делается работником подразделения, осуществляющего работу с клиентами, указанное в данном пункте разрешение не требуется, при условии, что скопированные данные / данные выписки не будут переданы лицам, не являющимися работниками этого подразделения.

12.13. Ответы на письменные запросы уполномоченных государственных органов, других организаций и учреждений о персональных данных Частных Клиентов, представителей Корпоративных Клиентов даются только с письменного согласия субъектов персональных данных, если иное не установлено законодательством. Ответы оформляются в письменном виде, на бланке Банка, и в том объеме, который позволяет не разглашать излишний объем персональных данных.

13. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЧАСТНОГО КЛИЕНТА ИЛИ ПРЕДСТАВИТЕЛЕЙ КОРПОРАТИВНОГО КЛИЕНТА

13.1. Работники Банка, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

13.2. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка обработки персональных данных Частных Клиентов, представителей Корпоративных Клиентов Банк вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

13.3. Банк возмещает субъекту персональных данных ущерб, причиненный неправомерным использованием Банком информации, содержащей персональные данные.

13.4. Неправомерный отказ в предоставлении собранных в установленном порядке документов, содержащих персональные данные Частных Клиентов или представителей Корпоративных Клиентов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации может повлечь наложение на должностных лиц Банка административного штрафа в размере, определяемом Кодексом Российской Федерации об административных правонарушениях.

Раздел V. ПОЛОЖЕНИЕ О МЕРАХ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о мерах по организации защиты информационных систем персональных данных в Банке устанавливает состав и содержание организационных и технических мер по обеспечению безопасности информационных систем персональных данных в Банке на протяжении всего цикла их создания и эксплуатации.

Меры по обеспечению безопасности персональных данных принимаются 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.

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой Банком в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

1.2. Положение о мерах по организации защиты информационных систем персональных данных в Банке разработано с учетом требований принятой в Банке Политики по защите персональных данных в Банке. Банк учитывает требования настоящего раздела при разработке и утверждении внутренних локальных актов и иных документов Банка, связанных с обработкой ПДн.

2. ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

2.1. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической и видео информации), общесистемное, прикладное, специальное программное обеспечение, а также средства защиты информации.

2.2. Для обеспечения защиты информации, содержащейся в информационной системе, Банком назначается уполномоченный сотрудник, ответственный за обеспечение безопасности информационных систем персональных данных.

2.3. Система защиты персональных данных включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

2.4. Выбор средств защиты информации для системы защиты персональных данных осуществляется Банком в соответствии с требованиями 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» (далее - Приказ ФСТЭК № 21), а также иными нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.

2.5. Определение типа угроз безопасности персональных данных, актуальных для информационных систем, производится Банком с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

2.6. Банк обеспечивает классификацию информационных систем в зависимости от того, какие категории персональных данных в ней обрабатываются и какие типы угроз актуальны для ИСПДн Банка. По результатам определяется набор требований, которые необходимо выполнить для обеспечения того уровня защищенности ПДн, который был определен при классификации ИСПДн Банка.

2.7. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных и контроль за выполнением требований к защите ПДн при обработке их в ИСПДн организуется и проводится Банком самостоятельно, не реже 1 раза в 3 года в сроки, определяемые Банком.

3. ОСНОВНЫЕ МЕРЫ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Состав и содержание организационных мер по обеспечению безопасности ПДн.

Необходимый уровень защищенности персональных данных при их обработке в информационных системах Банка обеспечивается принятием следующих основных организационных мер:

- 1) введение режима обеспечения безопасности помещений, в которых размещены ИСПДн Банка, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- 2) обеспечение безусловной сохранности носителей персональных данных;
- 3) назначение уполномоченного сотрудника, ответственного за обеспечение безопасности информационных систем персональных данных Банка;
- 4) утверждение перечня персональных данных и иных объектов, подлежащих защите в ИСПДн Банка;
- 5) утверждение перечня лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн Банка, необходим для выполнения ими служебных обязанностей;
- 6) проведение классификации ИСПДн Банка, по результатам которой определяется набор требований, необходимых для обеспечения достаточного уровня защищенности ПДн;
- 7) обеспечение проведения не реже 1 раза в 3 года проверки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, и осуществление регулярного контроля за выполнением требований к защите ПДн при обработке их в ИСПДн.

3.2. С учетом требований, перечисленных в пункте 2 настоящего раздела, проводятся следующие мероприятия:

- 1) Приказом Председателя Правления Банка назначается уполномоченный сотрудник, ответственный за обеспечение безопасности информационных систем персональных данных Банка. Разрабатывается и вводится в действие должностная инструкция, регламентирующая права и обязанности указанного сотрудника.
- 2) Вводится в действие приказ Председателя Правления Банка «О создании Комиссии по персональным данным» (далее по тексту – Комиссия по персональным данным).
- 3) Разрабатывается, утверждается и внедряется система организации доступа в помещения Банка, где осуществляется обработка ПДн, исключающая возможность несанкционированного доступа к техническим средствам обработки ПДн, хищения и нарушения работоспособности ИСПДн, хищения носителей информации ПДн.
- 4) Вводится в действие инструкция о порядке организации внутриобъектового и пропускного режимов в помещениях Банка.

- 5) Определяются состав и категории обрабатываемых в Банке персональных данных (результат оформляется в виде локального нормативного акта с перечнем персональных данных и иных объектов, подлежащих защите в Банке).
- 6) Разрабатывается и вводится в действие инструкция пользователя ИСПДн, регламентирующая права и обязанности работника Банка при работе с ИСПДн.
- 7) Разрабатывается и вводится в действие локальный нормативный акт, регламентирующий разграничение прав доступа к обрабатываемым в ИСПДн персональным данным.
- 8) Обеспечивается обучение работников Банка, осуществляющих обработку ПДн в информационных системах персональных данных, предусматривающее проведение не реже одного раза в год обучения пользованию средствами защиты информации, которые применяются в информационных системах Банка, правилам работы с ними, правилам обработки ПДн, в соответствии с утвержденными в Банке требованиями.
- 9) Разрабатывается и вводится в действие инструкция о порядке учета, использования, транспортировки, хранения и уничтожения в Банке съемных носителей персональных данных.
- 10) Обеспечивается учет съемных носителей ПДн в каждом структурном подразделении Банка (вводится в действие журнал учета съемных носителей ПДн).
- 11) Локальными актами, регламентирующими обработку и защиту персональных данных работников Банка, утверждаются перечни подразделений и работников, допущенных к обработке ПДн в информационных системах Банка.
- 12) Принимается локальный нормативный акт об ответственности работников Банка за разглашение персональных данных и несанкционированный доступ к персональным данным в информационных системах Банка.
- 13) Комиссией по персональным данным проводятся внутренние проверки и классификация ИСПДн Банка. Результаты оформляются в виде письменных отчетов, на основании которых разрабатывается план мероприятий по обеспечению безопасности ПДн в ИСПДн Банка.
- 14) Разрабатывается и утверждается план внутренних проверок состояния защиты ПДн в Банке. Вводится в действие журнал учета мероприятий по контролю соблюдения режима защиты персональных данных в информационных системах Банка.

3.3. Технические меры по обеспечению безопасности ПДн в ИСПДн.

Банк принимает технические меры по обеспечению безопасности информационных систем персональных данных.

План мероприятий по обеспечению защиты персональных данных в Банке включает следующие этапы работы:

- 1) определение на основании Приказа ФСТЭК № 21 базового набора мер по обеспечению безопасности персональных данных в ИСПДн Банка;
- 2) адаптация базового набора мер под ИСПДн Банка с учетом особенностей их функционирования, исключая те меры, которые связаны с информационными технологиями, не используемыми в ИСПДн;
- 3) уточнение списка мер с включением в него не выбранных ранее мер для нейтрализации актуальных угроз;
- 4) внедрение дополнительных мер, обеспечивающих выполнение требований к защите персональных данных, установленных нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

В составе мер, входящих в план мероприятий по обеспечению защиты персональных данных в Банке, в том числе, предусматривается:

- 1) внедрение системы парольной аутентификации работников Банка, допущенных к работе с ИСПДн, предусматривающей определение минимальной длины пароля, управление сроком действия и периодической сменой паролей; ограничение числа неудачных попыток входа в систему и использование программных генераторов паролей;
- 2) установление инструктивных и технических правил, обеспечивающих разграничение прав доступа работников к различным ПДн, находящимся в ИСПДн Банка;
- 3) разработка и внедрение регламента обеспечивающего установку и запуск в ИСПДн только разрешенного к использованию в информационной системе программного обеспечения, и исключающего возможность использования запрещенного к использованию в информационной системе программного обеспечения;
- 4) разработка инструкции, регламентирующей порядок резервирования и восстановления работоспособности программного обеспечения, баз данных и систем защиты ИСПДн;
- 5) внедрение технологий, позволяющих осуществлять резервирование и восстановление работоспособности программного обеспечения, баз данных и систем защиты ИСПДн;
- 6) разработка инструкции, регламентирующей модификацию программного обеспечения и технических средств информационной системы персональных данных;
- 7) внедрение технологий, позволяющих осуществлять сбор, запись, хранение, анализ, просмотр и защиту информации о событиях безопасности в ИСПДн Банка;
- 8) использование программного обеспечения по антивирусной защите, обеспечивающего обнаружение в ИСПДн вредоносных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования ПДн, иной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;
- 9) проведение систематических мероприятий по анализу защищенности ИСПДн и тестированию работоспособности системы защиты персональных данных;
- 10) обеспечение защиты ИСПДн, ее средств, систем связи и передачи данных при взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями;
- 11) разработка и ввод в действие электронного журнала учета обращений субъектов персональных данных о выполнении их законных прав, при обработке данных в ИСПДн.

3. ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Общее руководство деятельностью Банка по обеспечению безопасности ПДн осуществляет Председатель Правления Банка.

3.1. Председатель Правления Банка приказом назначает уполномоченного сотрудника, ответственного за обеспечение безопасности ИСПДн в Банке.

3.2. Уполномоченный сотрудник, ответственный за обеспечение безопасности ИСПДн в Банке, получает указания непосредственно от Председателя Правления Банка.

3.3. Уполномоченный сотрудник, ответственный за обеспечение безопасности ИСПДн в Банке, обязан не реже одного раза в три года проводить проверку состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных, при необходимости вносить предложения по доработке или модернизации системы защиты ПДн.

3.4. Председатель Правления приказом создает в Банке Комиссию по персональным данным, на которую возлагаются следующие обязанности:

- 1) реализация мероприятий, предусмотренных настоящим Положением;
- 2) осуществление внутреннего контроля и аудита соответствия практики обработки персональных данных в Банке тем требованиям и нормам, которые установлены Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», а также принятым в этой сфере иным нормативным правовым актам и требованиям к защите персональных данных, и локальным нормативным актам Банка;
- 3) организационное, методическое и научно-техническое руководство работами по созданию либо модернизации системы защиты ПДн.

3.5. Банк на договорной основе имеет право привлечь для разработки и внедрения систем защиты ПДн в ИСПДн Банка специализированные организации, имеющие лицензии ФСТЭК, ФСБ России на соответствующие виды деятельности.

4. ПОРЯДОК МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ПДн

5.1. Для ИСПДн, находящихся в эксплуатации, модернизация или доработка системы защиты ПДн должна проводиться в следующих случаях:

- 1) изменение состава или структуры самой ИСПДн или технических особенностей ее построения (изменение состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- 2) изменение состава угроз безопасности ПДн в ИСПДн;
- 3) изменение уровня защищенности, который необходимо обеспечить при защите ПДн.

4.1. Для определения необходимости доработки или модернизации систем защиты ПДн не реже одного раза в три года должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных. Проверка проводится уполномоченным сотрудником, ответственным за обеспечение безопасности ИСПДн. Результаты проверки оформляются Отчетом по проведению внутренней проверки и утверждаются Председателем Правления.

5. КОНТРОЛЬ СОБЛЮДЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ПДн

5.1. Уполномоченный сотрудник, ответственный за обеспечение безопасности ИСПДн, и Комиссия по персональным данным периодически (не реже одного раза в год) должны проводить проверку соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

5.2. В случае выявления фактов несоблюдения условий хранения носителей ПДн, или использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности ПДн, либо нарушения заданного уровня безопасности ПДн, должно в обязательном порядке проводиться служебное расследование (внутренняя проверка).

5.3. В процессе осуществления служебного расследования проводится разработка и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

5.4. По окончании проведения служебного расследования готовится заключение о лицах, виновных в выявленных нарушениях.

Раздел VI. ПОЛОЖЕНИЕ О НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий раздел разработан в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и устанавливает единый порядок неавтоматизированной обработки персональных данных в Банке.

1.2. Задачи, решаемые в процессе обработки персональных данных:

- документационное обеспечение обработки персональных данных;
- защита документированной информации, содержащей персональные данные.

2. ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных статьей 6 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;

- после направления уведомления об обработке персональных данных в Банке, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- после принятия необходимых мер по защите персональных данных.

2.2. В Банке приказом Председателя Правления назначается работник, ответственный за организацию обработки и защиту персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

2.3. Запрещается обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке.

3. СИСТЕМА ДОСТУПА К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ

3.1. Система доступа представляет собой совокупность норм и правил, определяющих порядок предоставления работникам прав доступа к документам, содержащим конфиденциальную информацию.

3.2. Система доступа должна отвечать следующим требованиям:

- доступ к конфиденциальным документам может предоставляться работникам, письменно оформившим с Банком соглашение о неразглашении ставших им известными конфиденциальных сведений. Письменное оформление соглашения о неразглашении конфиденциальной информации (соблюдения режима конфиденциальности) является обязательным условием для доступа работников к документам;

- доступ к конфиденциальным документам должен быть обоснованным, т.е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного работника;

- система доступа должна давать возможность обеспечения работников всеми необходимыми им в силу служебных обязанностей документами, но только теми, которые действительно необходимы для выполнения конкретного вида работ;

- доступ к документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению уполномоченного на то должностного лица. При этом соответствующее должностное лицо может давать разрешение на ознакомление с документами только входящими в сферу его деятельности и только установленному кругу лиц;

- доступ к документам осуществляется согласно должностной инструкции.

3.3. Доступ работников Банка к конфиденциальной информации осуществляется на добровольной основе. Эти отношения устанавливаются при приеме гражданина на работу или уже в ходе трудовых отношений. При этом соблюдаются следующие условия:

- ознакомление работника под роспись с перечнем конфиденциальной информации;

- ознакомление работника под роспись с установленным в Банке режимом по охране конфиденциальности и с мерами ответственности за его нарушение;

- создание работнику необходимых условий для соблюдения им установленного режима по охране конфиденциальности.

3.4. Доступ работников Банка к персональным данным осуществляется в соответствии с Перечнем работников, допущенных к обработке персональных данных в Банке.

3.5. Работник принимает следующие обязательства:

- по соблюдению установленного в Банке режима по охране конфиденциальной информации;

- о неразглашении конфиденциальной информации, ставшей ему известной в период выполнения трудовых отношений, после прекращения трудового договора в течение срока, предусмотренного в Соглашении о неразглашении конфиденциальной информации и не использовании этой информации в личных целях;

- о возмещении причиненного ущерба, если работник виновен в разглашении конфиденциальной информации, ставшей ему известной в связи с выполнением им трудовых обязанностей (в том числе после прекращения трудового договора);

- о возврате при прекращении или расторжении трудового договора всех имеющихся у работника материальных носителей конфиденциальной информации.

4. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

4.1. На бумажных носителях:

4.1.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных и магнитных носителях.

4.1.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

4.1.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

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

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

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) 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;

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

4.1.5. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на объекты Банка или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом Банка, содержащим 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, на которой находится оператор, 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 объекты Банка.

4.1.6. 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 отдельной 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.

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

4.1.8. Правила, предусмотренные пунктами 4.1.6 и 4.1.7 настоящего раздела, применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

4.1.9. 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.

4.2. В электронном виде без использования средств автоматизации:

4.1.1. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на электронных носителях информации.

4.1.2. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

4.1.3. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от иных зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных

осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

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

5. ПОДГОТОВКА И УЧЕТ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Бланки типовых форм документов (справки, карточки, талоны, ведомости и т.п.) могут изготавливаться при помощи средств вычислительной техники или на компьютере.

5.2. Персональные данные (переменная часть) в типовые формы документов вносятся при помощи средств вычислительной техники, рукописным способом.

5.3. После внесения переменной части в типовые формы, последние становятся документами и подлежат немедленному учету в журнале изданных документов с присвоением им учетного номера.

6. ПОЛУЧЕНИЕ (ОТПРАВЛЕНИЕ) ДОКУМЕНТОВ И ИХ УЧЕТ

6.1. Все документы, поступающие из иных организаций, подлежат регистрации в журнале учета поступивших документов. На самом документе в правом нижнем углу первого листа документа проставляется отметка о поступлении, которая содержит входящий номер, присвоенный документу, дату поступления.

6.2. Пересылка документов может осуществляться через органы специальной связи или через почтовое отделение связи.

6.3. Об отправленных документах производятся соответствующие отметки в учетных формах.

7. КОПИРОВАНИЕ ДОКУМЕНТОВ

7.1. При действительной служебной необходимости в дополнительных экземплярах документов производится их копирование.

7.2. На некоторых документах может стоять отметка о том, что снятие копий с этого документа не разрешается. Такие документы копированию не подлежат.

7.3. Разрешение на копирование (снятие копий) документов могут давать соответствующие должностные лица (руководители структурных подразделений), наделенные правом распоряжения сведениями.

7.4. Разрешение на изготовление дополнительных экземпляров (копий) учетного документа оформляется на обороте последнего листа экземпляра, с которого производится копирование. В разрешении указываются номера документов или страниц, с которых необходимо сделать копию, а также количество копий.

8. РЕЖИМ СОХРАННОСТИ ДОКУМЕНТОВ

8.1. Организация хранения документов предполагает, что помещения, где хранятся документы, должны соответствовать требованиям технической безопасности, противопожарной безопасности, а также установленным санитарным нормам.

8.2. Для обеспечения физической сохранности документов, дел, а также для предотвращения разглашения содержащейся в них информации устанавливается специальный режим их хранения и обращения.

8.3. Право входа в такие помещения имеют Председатель Правления Банка и работники, имеющие прямое отношение к обработке и хранению документов.

Раздел VII. НОРМАТИВНЫЕ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ

При организации и проведении работ по обеспечению безопасности ПДн в Банке работники Банка должны руководствоваться следующими нормативными и методическими документами:

1. Конституция Российской Федерации (часть 1 статьи 23, статья 24);
2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
5. Федеральный закон от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматической обработке персональных данных»;
6. Указ Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
7. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
8. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
9. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
10. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

СОГЛАСИЕ
Работника на обработку персональных данных

Я, _____,
(Ф.И.О. работника)

зарегистрированный (ая) по адресу: _____,

паспорт серия _____ № _____, выдан _____

«___» _____ 20__ г., в соответствии со ст. 9 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» даю согласие на обработку своих персональных данных КБ «Байкалкредобанк» (ПАО) (далее - Оператор), расположенному по адресу: 664025, Иркутская обл., г. Иркутск, ул. Ленина, д. 18, а именно: совершение действий, предусмотренных п. 3 ст. 3 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», со всеми данными, которые находятся в распоряжении Оператора.

1. Перечень персональных данных, на обработку которых дается согласие:

- фамилия, имя, отчество (в т.ч. предыдущие),
- паспортные данные или данные иного документа, удостоверяющего личность,
- дата рождения, место рождения,
- гражданство,
- отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения,
- данные документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке,
- данные документов о подтверждении специальных знаний,
- данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений, сведения о наградах и званиях,
- знание иностранных языков,
- семейное положение и данные о составе и членах семьи,
- сведения о социальных льготах, пенсионном обеспечении и страховании,
- данные документов об инвалидности (при наличии),
- данные медицинского заключения (при необходимости),
- стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке,
- должность, квалификационный уровень,
- сведения о заработной плате (доходах), банковских счетах, картах,
- адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства,
- номера телефонов (стационарный домашний, мобильный),
- данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (при наличии),
- данные страхового свидетельства государственного пенсионного страхования,
- данные страхового медицинского полиса обязательного страхования граждан,
- личная фотография,
- иные сведения, с которыми Работник считает нужным ознакомить Оператора, либо дополнительная информация необходимая Оператору.

2. Цели обработки:

Вышеуказанные персональные данные предоставляю для обработки в целях соблюдения требований трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, продвижении по службе, обеспечения личной безопасности, контроля объема и качества выполняемой работы, обеспечения сохранности имущества и организационной деятельности Оператора.

3. Перечень действий, на совершение которых дается согласие:

Разрешаю Оператору производить с моими персональными данными действия (операции), определенные статьей 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», а именно: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

4. Согласие на передачу персональных данных третьим лицам:

Разрешаю обмен (прием, передачу, обработку) моих персональными данными между Оператором (Банком) и третьими лицами в соответствии с заключенными договорами и соглашениями, в целях соблюдения моих законных прав и интересов.

5. Сроки обработки и хранения персональных данных:

Обработка персональных данных прекращается после окончания трудового договора работника. В дальнейшем бумажные носители персональных данных находятся на архивном хранении (постоянно или 75 лет), а персональные данные работников на электронных носителях удаляются из информационной системы.

Согласие на обработку данных (полностью или частично) может быть отозвано субъектом персональных данных на основании его письменного заявления.

Права и обязанности в области защиты персональных данных мне разъяснены.

С Положением об обработке и защите персональных данных Оператора ознакомлен(а).

Настоящее согласие действует с момента его подписания.

«__» _____ 20__ г.

(подпись)

СОГЛАСИЕ

на обработку персональных данных (кредитный отдел)

г. Иркутск

«__» _____ 20__ г.

Я, _____,
(фамилия, имя, отчество)

зарегистрированный(ная) по адресу:

_____,
паспорт: серия _____ № _____, выдан _____,
«__» _____ 20__ г., в соответствии с требованиями ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» подтверждаю свое согласие Коммерческому Банку «Байкалкредобанк» (публичное акционерное общество) (КБ «Байкалкредобанк» (ПАО)), (далее - Оператор), расположенному по адресу: 664025, г. Иркутск, ул. Ленина, 18, на обработку моих персональных данных, а именно: фамилия, имя, отчество, паспортные данные, включая номер паспорта, сведения о дате выдачи и выдавшем паспорт органе, дата рождения, место рождения, пол, адрес регистрации, данные паспорта или иного документа, удостоверяющего личность иностранного гражданина, включая номер, сведения о дате выдачи и выдавшем органе, срок действия, дата рождения, пол, данные миграционных документов иностранного гражданина или лица без гражданства: визы, миграционной карты, уведомления Федеральной миграционной службы о месте пребывания, гражданство, адрес регистрации иностранного гражданина в стране, гражданином которой он/она является, адрес местонахождения (места пребывания), контактная информация, включая номера телефонов, факсов, e-mail, образование, занимаемая(ые) должность(и), сведения о трудовой деятельности, семейное положение, состав семьи, данные свидетельства о рождении ребенка, данные свидетельства о заключении брака, сведения о близких родственниках, социальное положение, имущественное положение, сведения о доходах и их источниках, идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования, номер счёта в иных кредитных организациях, иные сведения, связанные с получением услуг, оказываемых Оператором, в том числе связанные с рассмотрением заявки на предоставление кредита, заключением с Оператором и дальнейшим исполнением Кредитного договора и сопутствующих ему договоров, обеспечивающих надлежащее исполнение Кредитного договора, принятием решений или совершением иных действий, порождающих юридические последствия в отношении меня или других лиц, предоставлением мне информации об оказываемых Оператором услугах.

Предоставляю Оператору право осуществлять любое действие (операцию) 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.

Я ознакомлен(а), что:

- 1) согласие на обработку персональных данных действует с даты подписания настоящего согласия до достижения цели обработки персональных данных;
- 2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;
- 3) в случае отзыва согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- 4) персональные данные хранятся у Оператора в течение установленного законодательством Российской Федерации срока хранения документов.

Я признаю и подтверждаю, что:

- в случае необходимости предоставления персональных данных для достижения указанных выше целей третьему лицу, а равно как при привлечении третьих лиц к оказанию услуг в указанных целях, передаче Оператором принадлежащих ему функций и полномочий иному лицу, Оператор вправе в необходимом объёме раскрывать для совершения вышеуказанных действий информацию обо мне лично (включая мои персональные данные) таким третьим лицам, их агентам и иным уполномоченным ими лицам, а также предоставлять таким лицам соответствующие документы, содержащие такую информацию;

- настоящее согласие считается данным мною любым третьим лицам, указанным выше, с учётом соответствующих изменений, и любые такие третьи лица имеют право на обработку персональных данных на основании настоящего согласия.

«__» _____ 20__ г.

_____ (подпись)

_____ (расшифровка подписи)

СОГЛАСИЕ
на обработку персональных данных (открытие счета)

г. Иркутск

«__» _____ 20__ г.

Я, _____,
(фамилия, имя, отчество)

зарегистрированный(ная) по адресу:

паспорт: серия _____ № _____, выдан _____
«__» _____ 20__ г., в соответствии с требованиями ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» подтверждаю свое согласие Коммерческому Банку «Байкалкредобанк» (публичное акционерное общество) (КБ «Байкалкредобанк» (ПАО)), (далее - Оператор), расположенному по адресу: 664025, г. Иркутск, ул. Ленина, 18, на обработку моих персональных данных, включающих: фамилия, имя, отчество, год рождения, месяц рождения, место рождения, телефон, электронная почта, паспортные данные или данные иного документа, удостоверяющего личность, иные сведения, связанные с получением услуг, оказываемых Оператором, в том числе связанные с открытием счета, осуществлением валютно-обменных операций, переводом без открытия счета, открытием счета/вклада, открытием счета для осуществления банковских операций с использованием пластиковой карты.

Предоставляю Оператору право осуществлять любое действие (операцию) 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.

Я ознакомлен(а), что:

- 1) согласие на обработку персональных данных действует с даты подписания настоящего согласия до достижения цели обработки персональных данных;
- 2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;
- 3) в случае отзыва согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- 4) персональные данные хранятся у Оператора в течение установленного законодательством Российской Федерации срока хранения документов.

Я признаю и подтверждаю, что:

- в случае необходимости предоставления персональных данных для достижения указанных выше целей третьему лицу а равно как при привлечении третьих лиц к оказанию услуг в указанных целях, передаче Оператором принадлежащих ему функций и полномочий иному лицу, Оператор вправе в необходимом объеме раскрывать для совершения вышеуказанных действий информацию обо мне лично (включая мои персональные данные) таким третьим лицам, их агентам и иным уполномоченным ими лицам, а также предоставлять таким лицам соответствующие документы, содержащие такую информацию;
- настоящее согласие считается данным мною любым третьим лицам, указанным выше, с учётом соответствующих изменений, и любые такие третьи лица имеют право на обработку персональных данных на основании настоящего согласия.

«__» _____ 20__ г.

(подпись)

(расшифровка подписи)

ОТЗЫВ СОГЛАСИЯ
на обработку персональных данных

Я, _____,

в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" отзываю у КБ «Байкалкредобанк» (ПАО) согласие на обработку моих персональных данных.

Прошу прекратить обработку моих персональных данных в связи с

(указать причину)

в срок, не превышающий тридцати дней с момента поступления настоящего отзыва.

« ___ » _____ 20__ г.

(подпись)

(расшифровка подписи)

РАЗЪЯСНЕНИЕ

субъекту персональных данных юридических последствий
отказа от предоставления своих персональных данных

Уважаемый(ая) _____

В соответствии с частью 2 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» разъясняем, что обязанность предоставления Вами персональных данных установлена

(указывается пункт Федерального закона, его реквизиты и наименование)

а также следующими нормативными актами:

(указываются реквизиты и наименования нормативных актов)

В случае Вашего отказа предоставить свои персональные данные _____ не сможет на законных основаниях осуществить

(указывается действие)

что приведет к следующим для Вас юридическим последствиям:

(перечисляются юридические последствия для субъекта, т.е. случаи возникновения, изменения или прекращения личных либо имущественных прав гражданина или случаи, иным образом затрагивающие его права, свободы и законные интересы)

С уважением,

(подпись)

(расшифровка подписи)

СОГЛАШЕНИЕ № _____
о неразглашении конфиденциальной информации

г. Иркутск

« ____ » _____ 20__ г.

КБ «Байкалкредобанк» (ПАО), именуемый в дальнейшем «Банк», в лице Председателя Правления Геряева Алексея Николаевича, действующего на основании Устава, с одной стороны, и

(ФИО)

зарегистрированный(-ая) по адресу: г. Иркутск, ул. _____, д. ____, кв. ____,
паспорт РФ: серия _____ № _____, выдан « ____ » _____ 20__ г.,

именуемый(-ая) в дальнейшем «Работник», с другой стороны, совместно именуемые в дальнейшем «Стороны», заключили настоящее соглашение о нижеследующем.

1. Работник в связи с исполнением своих должностных обязанностей получает доступ к персональным данным сотрудников Банка, клиентов Банка и их представителей, иных лиц, а также к сведениям, содержащим иную конфиденциальную информацию, доступ к которым ограничен Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и иными правовыми актами, и **обязуется не разглашать ставшие ему известными персональные данные сотрудников, клиентов Банка и их представителей, иных лиц, иные сведения, содержащие конфиденциальную информацию**, за исключением случаев, предусмотренных законодательством Российской Федерации.

2. Под конфиденциальной информацией в настоящем соглашении понимается речевая, аудиовизуальная, документированная информация с ограниченным доступом и иная информация, содержащая охраняемую в соответствии с действующим законодательством тайну Банка, а также персональные данные сотрудников, клиентов Банка и их представителей, иных лиц. Конфиденциальная информация, содержащаяся в локальной сети Банка, также имеет ограниченный доступ.

К конфиденциальной информации по настоящему соглашению в частности, но не ограничиваясь, относится любая или вся, настоящая или будущая, техническая, финансовая, деловая информация, статистика, данные, схемы, планы, спецификации, документы, идеи, концепции, продукты, процессы, технологии, цены, пароли доступа к информационным системам и другая информация, которая отнесена к конфиденциальной действующим законодательством Российской Федерации и локальными правовыми актами Банка и была передана Работнику для выполнения последним своих трудовых обязанностей.

3. Не могут являться конфиденциальной информацией сведения:

- которые до момента заключения настоящего соглашения были публично обнародованы;
- которые стали общедоступны во время действия настоящего соглашения, но без виновного участия Работника.

4. Вся конфиденциальная информация, полученная Работником в материальной (схемы, рисунки, письма, фотографии и пр.) и нематериальной формах, является собственностью Банка и используется только на условиях настоящего соглашения.

5. Работник обязуется:

5.1. Знать требования Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Положения «Об обработке и защите персональных данных» Банка, Положения «О конфиденциальной информации и коммерческой тайне» Банка.

5.2. Не разглашать и не передавать третьим лицам сведения, являющиеся конфиденциальной информацией, ставшие ему известными в связи с исполнением трудовых обязанностей, а также защищать вышеуказанные сведения от посягательств и попыток ее обнародования третьими лицами.

5.3. Использовать сведения, полученные при исполнении своих трудовых обязанностей, лишь в интересах Банка.

5.4. В случае увольнения из Банка вернуть все сведения, полученные на материальных носителях, а также их копии, в течение одного дня с момента получения соответствующего требования о возврате.

5.5. Не использовать конфиденциальную информацию после увольнения из Банка.

6. В случае разглашения Работником сведений, являющихся конфиденциальной информацией, трудовой договор с Работником подлежит расторжению в соответствии с подпунктом «в» пункта 6 статьи 81 Трудового кодекса Российской Федерации.

7. В случае разглашения сведений, являющихся конфиденциальной информацией, Работник обязан в полном объеме возместить понесенные в результате такого разглашения убытки Банка.

8. В случае разглашения конфиденциальной информации Работник может быть привлечен к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

9. Настоящее соглашение действует бессрочно. Прекращение отношений по трудовому договору не является основанием для прекращения обязательств Сторон по настоящему соглашению.

10. Настоящее соглашение составлено в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, по одному для каждой из Сторон.

Председатель Правления
КБ «Байкалкредобанк» (ПАО)

Работник

_____ А.Н. Геряев

_____ / _____

М.П.

Акт приема-передачи
документов (иных материальных носителей),
содержащих персональные данные Работника

г. Иркутск

«__» _____ 20__ г.

Во исполнение договора оказания услуг № ____ от «__» _____ 20__ года, заключенного между КБ «Байкалкредобанк» (ПАО), именуемым далее «Заказчик», в лице _____, действующего на основании _____, и _____, именуемым в дальнейшем «Исполнитель», в лице _____, действующего на основании _____, составили настоящий акт приема-передачи документов (иных материальных носителей), содержащих персональные данные Работника, о нижеследующем:

ЗАКАЗЧИК передает, а ИСПОЛНИТЕЛЬ принимает документы (иные материальные носители), содержащие персональные данные Работника Заказчика, на срок _____ и в целях: _____.

**Перечень документов (иных материальных носителей),
содержащих персональные данные Работника**

№ п/п	Наименование	Количество
Всего:		

Полученные персональные данные Работника могут быть использованы лишь в целях, для которых они сообщены. Незаконное использование предоставленных персональных данных путем их разглашения, уничтожения или использования другими способами, установленными федеральными законами, может повлечь соответствующую гражданско-правовую, материальную, дисциплинарную, административно-правовую и уголовную ответственность.

Передал

(Ф.И.О., должность лица, осуществляющего передачу персональных данных Работника)

(Подпись)

Принял

(Ф.И.О., должность лица, принимающего документы (иные материальные носители), содержащих персональные данные Работника)

(Подпись)

Акт № _____
об уничтожении носителей, содержащих персональные данные

г. Иркутск

«___» _____ 20__ г.

Комиссия в составе:

Председатель – _____

Члены комиссии – _____

провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных и иной конфиденциальной информации (далее носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежат гарантированному уничтожению. Комиссия составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

№ п/п	Дата	Тип носителя	Учетный номер носителя	Категория информации	Примечание

Всего носителей - _____ (_____) штук.
(количество - цифрами и прописью)

На указанных носителях персональные данные уничтожены путем

(стирания на устройстве/гарантированного уничтожения информации /иного способа)

Перечисленные носители персональных данных уничтожены путем

*(разрезания/сжигания/размагничивания/физического уничтожения/
механического уничтожения /иного способа)*

Председатель комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /
_____ / _____ /

ПРИЛОЖЕНИЕ № 11

к Положению об обработке и
защите персональных данных
КБ «Байкалкредобанк» (ПАО)

Журнал
учета съемных носителей конфиденциальной информации
(персональных данных)

№ п / п	Регистрационный номер/ дата	Тип/ёмкость машинного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место установки (использования)/дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)
1									
2									
3									
...									
N									

СОГЛАСИЕ

на обработку персональных данных, необходимых для регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, и иных сведений, если такие сведения предусмотрены федеральными законами в указанной системе, и биометрических персональных данных гражданина Российской Федерации в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации

Я, _____,

(фамилия, имя, отчество (при наличии) полностью)

паспорт серия _____ N _____ выдан _____

(кем и когда выдан документ)

проживающий (проживающая) по адресу: _____

1. Свободно, своей волей и в своем интересе даю конкретное, информированное и сознательное согласие на обработку следующих моих персональных данных:

а) фамилия, имя, отчество (при наличии), пол, гражданство, дата и место рождения, номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе, адрес регистрации по месту жительства (пребывания), идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, контактные данные (номер абонентского устройства подвижной радиотелефонной связи, адрес электронной почты), иные сведения, предусмотренные федеральными законами, а также необходимые для размещения данных в моей учетной записи в федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (далее - единая система идентификации и аутентификации);

б) изображение лица, полученное с помощью фото- и видеоустройств, голос, полученный с помощью звукозаписывающих устройств, которые требуются для подтверждения моей идентификации с применением единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее - единая биометрическая система) в соответствии с законодательством Российской Федерации.

2. Свободно, своей волей и в своем интересе даю конкретное, информированное и сознательное согласие на обработку моих персональных данных, указанных в пункте 1 настоящего согласия, в целях моей идентификации с применением информационных технологий:

а) Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации - оператору единой системы идентификации и аутентификации (Россия, 125375, г. Москва, ул. Тверская, д. 7) - на обработку (включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) персональных данных, указанных в подпункте "а" пункта 1 настоящего согласия, в том числе обработку моих персональных данных при предоставлении государственных и муниципальных услуг;

б) публичному акционерному обществу междугородной и международной электрической связи "Ростелеком" - оператору единой биометрической системы (Россия, 115172, г. Москва, ул. Гончарная, д. 30, стр. 1) - на обработку (включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ) в том числе результата обработки моих персональных данных, обезличивание, блокирование, удаление, уничтожение) персональных данных, указанных в подпункте "б" пункта 1 настоящего согласия;

в) лицу, уполномоченному на обработку персональных и биометрических персональных данных в соответствии с законодательством Российской Федерации, _____,

(полное наименование юридического лица)

находящемуся _____,

(адрес местонахождения юридического лица)

на обработку (включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных) персональных данных, биометрических персональных данных, в том числе

передачу данных, указанных в подпункте "а" пункта 1 настоящего согласия, оператору единой системы идентификации и аутентификации, указанному в подпункте "а" пункта 2 настоящего согласия, а также передачу данных, указанных в подпункте "б" пункта 1 настоящего согласия, оператору единой биометрической системы, указанному в подпункте "б" пункта 2 настоящего согласия.

Лица, указанные в подпунктах "а" - "в" пункта 2 настоящего согласия, вправе осуществлять автоматизированную обработку персональных данных, указанных в пункте 1 настоящего согласия, или их обработку без использования средств автоматизации, в том числе с передачей по каналам связи, защита которых обеспечивается путем реализации соответствующих правовых, организационных и технических мер, предусмотренных законодательством Российской Федерации о защите персональных данных.

3. Для достижения цели, указанной в пункте 2 настоящего согласия:

- даю согласие лицам, указанным в подпунктах "а" - "в" пункта 2 настоящего согласия, на проверку предоставленных мной сведений на предмет их полноты и достоверности, в том числе с использованием государственных и муниципальных информационных систем и ресурсов, а также путем направления указанными лицами запросов в иные органы и организации;

- соглашаюсь с тем, что лица, указанные в подпунктах "а" - "в" пункта 2 настоящего согласия, вправе поручить обработку моих персональных данных, указанных в пункте 1 настоящего согласия, другому лицу (лицам):

(наименование или фамилия, имя, отчество (при наличии) и адрес)

на основании поручения либо заключаемого с этим лицом (лицами) договора, в том числе государственного контракта, либо путем принятия государственным органом соответствующего акта (далее - поручение оператора).

Я проинформирован, что ответственность передо мной за действия лица, обрабатывающего мои персональные данные по поручению оператора, несет оператор, выдавший соответствующее поручение.

4. Подтверждаю, что даю согласие на обработку моих персональных данных, указанных в пункте 1 настоящего согласия, лицам, указанным в подпунктах "а" - "в" пункта 2 настоящего согласия.

5. Настоящее согласие действует со дня его подписания до дня его отзыва, но не более 50 лет.

6. Подтверждаю, что проинформирован (проинформирована) о возможности отзыва настоящего согласия на основании положений Федерального закона "О персональных данных" путем личного обращения или направления письменного обращения (в том числе в форме электронного документа, подписанного простой электронной подписью или усиленной квалифицированной электронной подписью), на имя лиц, указанных в подпунктах "а" - "в" пункта 2 настоящего согласия, в том числе я проинформирован (проинформирована), что имею право:

- отозвать настоящее согласие в целях прекращения обработки лицом, указанным в подпункте "в" пункта 2 настоящего согласия, как всех указанных в пункте 1 настоящего согласия персональных данных, так и отдельно биометрических персональных данных, указанных в подпункте "б" пункта 1 настоящего согласия;

- отозвать настоящее согласие в целях прекращения обработки в единой системе идентификации и аутентификации персональных данных, указанных в подпункте "а" пункта 1 настоящего согласия;

- отозвать настоящее согласие в целях прекращения обработки в единой биометрической системе биометрических персональных данных, указанных в подпункте "б" пункта 1 настоящего согласия.

7. Я проинформирован (проинформирована), что лица, указанные в подпунктах "а" - "в" пункта 2 настоящего согласия, вправе после получения отзыва настоящего согласия, а равно после истечения срока действия настоящего согласия, продолжать обработку моих персональных данных при наличии оснований, предусмотренных частью 2 статьи 9 Федерального закона "О персональных данных".

" ____ " _____ 20__ г.

(подпись)

(фамилия, имя, отчество)