Приложение № 1
к Приказу от 13 марта 2018 г. № 50

ПОЛОЖЕНИЕ

о порядке обработки и защите персональных данных в АО КБ «АГРОПРОМКРЕДИТ»

г. Лыткарино,
Московская область
2018 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о порядке обработки и защите персональных данных в АО КБ «АГРОПРОМКРЕДИТ» (далее – Положение) устанавливает общие требования к организации обработки и обеспечению безопасности персональных данных в АО КБ «АГРОПРОМКРЕДИТ» (далее – Банк).

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон №152-ФЗ), другими федеральными законами и нормативными правовыми актами законодательства РФ («Нормативные ссылки» представлены в Приложение №8 Положения), а также в соответствии с Уставом Банка и действующими внутрибанковскими нормативными актами.

1.3. Настоящее Положение определяет основные требования к порядку обработки (как с использованием средств автоматизации, так и без использования таковых), к обеспечению безопасности персональных данных Сотрудников, родственников Сотрудников, Клиентов, Управления Банка и Иных лиц, обязанности и ответственность лиц, участвующих в обработке персональных данных, а также порядок взаимодействия структурных подразделений Банка в целях обеспечения указанных требований.

1.4. Действия настоящего Положения распространяются и являются обязательными для выполнения всеми Сотрудниками и иными лицами, имеющими договорные отношения с Банком, при этом срочность и важность выполняемых ими работ не должны являться основанием для нарушения требований настоящего Положения и других документов, регламентирующих вопросы обработки и защиты персональных данных.

1.5. Настоящий документ не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов, имеющих статус архивных документов в соответствии с действующим законодательством об архивном деле в РФ.

1.6. Настоящее Положение доводится в Банке до сведения всех Сотрудников, участвующих в обработке персональных данных под роспись.

1.7. В настоящем документе используются следующие термины и определения:

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

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

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

Категории субъектов персональных данных:

1) Сотрудники - физические лица, вступившие в трудовые отношения с Банком;

2) Родственники сотрудников - физические лица, обработка данных которых осуществляется с целью выполнения трудового законодательства в отношении Сотрудников;

3) Клиенты (представители Клиентов) – физические лица с которыми Банк взаимодействует в рамках гражданско-правовых договоров на оказание услуг, предоставляемых Банком;

4) Управление Банка – лица, к которым относятся:

– физические лица - руководители, члены органов управления, акционеры, участники, действующие на основании документов, оформленных согласно законодательству РФ, данные которых предоставляются в целях заключения и исполнения договоров с Банком;

– физические лица, не являющиеся сотрудниками Банка: члены органов управления Банка, аффилированные лица, иные физические лица, обязанность раскрытия информации о которых возложена на Банк законодательством РФ.

5) Иные лица – лица, к которым относятся:

– физические лица и представители физических, юридических лиц, индивидуальных предпринимателей и иных лиц, занимающихся частной практикой, данные которых обрабатываются в целях заключения и исполнения договоров с Банком;

– физические лица - выгодоприобретатели по договорам, заключаемым между Клиентами и Банком.

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

Конфиденциальность информации (в том числе персональные данные) - обязательное для выполнения лицом (или организацией), получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Материальный носитель информации - материальный объект, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов:

- машинный носитель информации – любое техническое устройство либо физическое поле, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации.

- бумажный носитель информации - материальный объект на бумажной основе, в котором отображается информация в виде символов или образов.

Несанкционированный доступ/несанкционированные действия (НСД) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и/или правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по функциональным и техническим характеристикам.

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

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

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 распространяется требование обязательной публикации информации.

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

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

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

Представитель - лицо, которое наделено правом представлять интересы субъекта персональных данных в силу специального указания закона или лицо, представляющее субъекта персональных данных, действующее на основании поручения (доверенности или иного документа) удостоверенного (удостоверенной) нотариально, или заверенного (заверенной) способами, приравненными к нотариальному заверению.

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

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу («трансграничная передача персональных данных» в Банке не осуществляется).

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

2. ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Состав обрабатываемых персональных данных определяется в зависимости от целей обработки и может включать следующие сведения:

1. Фамилия, имя, отчество (в т.ч. прежние), пол, дата, год и место рождения, степень родства.
2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

3. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.

4. Номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства (по паспорту).

5. Сведения об образовании, квалификации, о знании иностранных языков и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения).

6. Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончанию образовательного учреждения и другие сведения).

7. Фотографии сотрудников Банка на Личном листке по учету кадров, на удостоверении сотрудника Банка и в общедоступных источниках Банка (в т.ч. в электронном виде), данные в устройствах, ксерокопии с документов, удостоверяющих личность и имеющих фотографию владельца, записи внутренних видеосистем, предназначенных для обеспечения банковской и личной безопасности субъектов персональных данных. При этом видеоматериалы системы видеонаблюдения не являются биометрическими персональными данными, так как характеристики оборудования не позволяют получать видеозаписи с привязкой к конкретному субъекту персональных данных.

8. Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения).

9. Сведения о номере, серии и дате выдачи Трудовой книжки (вкладыша в нее) и записях в ней.

10. Содержание и реквизиты трудового договора с Сотрудником Банка или гражданско-правового договора с гражданином.

11. Сведения о заработной плате (номера счетов для расчета с сотрудниками, данные зарплатных договоров с Клиентами, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, налогам и другие сведения).

12. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на(с) учет(а) и другие сведения).

13. Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долговым обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения).

14. Сведения об имуществе (имущественном положении).

15. Автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств).

16. Недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость, полные адреса размещения объектов недвижимости и другие сведения).

17. Банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов, вид, срок размещения, сумма, условия вклада и другие сведения).

18. Кредиты (займы), банковские счета (в том числе спецкартсчета), денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, спецкартсчетов, номера банковских карт, кодовая информация по банковским картам, коды кредитных историй, адреса приобретаемых объектов недвижимости, сумма и валюта кредита или займа, цель кредитования, условия кредитования, сведения о залоге, сведения о приобретаемом объекте, данные по ценным бумагам, остатки и суммы движения по счетам, тип банковских карт, лимиты и другие сведения).

19. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

20. Сведения об идентификационном номере налогоплательщика.

21. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

22. Сведения, указанные в оригиналах и копиях приказов по личному составу Банка и материалах к ним.

23. Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) сотрудников Банка.

24. Материалы по аттестации и оценке сотрудников Банка.

25. Материалы по внутренним служебным расследованиям в отношении сотрудников Банка.

26. Внутрибанковские материалы по разбирательству и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами.

27. Сведения о временной нетрудоспособности Сотрудника Банка.

28. Табельный номер сотрудника Банка.

29. Сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения).

30. Сведения о миграционной карте, а также сведения о документе, подтверждающем право пребывания в РФ иностранного гражданина.

31. Полномочия по представлению интересов юридического лица.

32. Номер пенсионного удостоверения.

33. Адрес электронной почты.

34. Данные документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в РФ.

3. ЦЕЛЬ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Осуществление возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым и Трудовым кодексами Российской Федерации, Федеральными законами, в частности: «О банках и банковской деятельности», «Об акционерных обществах», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «О страховании вкладов физических лиц в банках Российской Федерации», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», регулируется нормативными актами Банка России, а также Уставом и нормативными актами Банка.

3.2 Организация учета сотрудников Банка для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия сотруднику в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами осуществляется в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также Уставом и нормативными актами Банка.

3.3 Продвижение товаров, работ и услуг Банка и его партнеров на рынке путем осуществления прямых контактов с физическими лицами с помощью средств связи.

3.4 Обеспечение безопасности жизни и имущества различных категорий субъектов персональных данных, находящихся на территории Банка.

4. ПРАВИЛА ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Список лиц, допущенных к обработке персональных данных (далее - Список), включающий сотрудников Банка, использующих в работе персональные данные субъектов персональных данных и отвечающих за их сохранность при обработке в соответствии с законодательством Российской Федерации, определяется Департаментом по экономической безопасности и режиму (далее – ДЭБиР) и утверждается Председателем Правления Банка.

4.2. Допуск сотрудников к обработке персональных данные предоставляется после выполнения следующих мероприятий:

– ознакомления под подпись с руководящими документами Банка по обработке и защите персональных данных;

– оформления письменного обязательства о неразглашении персональных данных (Приложение № 1 к настоящему Положению).

4.3. Управлению по работе с персоналом Банка, в филиалах – специалистам по работе с персоналом или лицам, исполняющим обязанности по работе с персоналом, необходимо

подавать информацию (Приложение № 7 к настоящему Положению) в Управление технических средств безопасности и режима ДЭБиР Банка. В случае изменения Штатного расписания или при приеме/переводе сотрудника (в том числе по заключении/расторжении Договора подряда) - в течение недели с момента изменений, в случае увольнения или декретного отпуска сотрудника - не более трех рабочих дней с даты поступления заявления об увольнении/декретном отпуске сотрудника.

4.4. Сотрудники Банка, имеющие доступ к персональным данным, выполняют действия по обработке персональных данных в соответствии со служебной необходимостью и возложенными на них функциями в рамках должностных инструкций.

4.5. Доступ в ИСПДн предоставляется путем наделения прав доступа к соответствующим ресурсам и прикладному программному обеспечению, обрабатывающему персональные данные.

4.6. Лица, получившие доступ к персональным данным, должны хранить в тайне известные им сведения конфиденциального характера и информировать ДЭБиР, в филиалах – Службу экономической безопасности (далее - СЭБ) в случае утечки/утраты персональных данных, о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к персональным данным.

4.7. Лица, получившие доступ к персональным данным, должны использовать эти сведения лишь в целях, для которых они сообщены, соблюдая требования законодательства РФ и локальных актов Банка. Данные лица имеют право доступа только к тем персональным данным, обработка которых предусмотрена их должностными обязанностями.

4.8. В трудовых договорах с Сотрудниками Банка и в договорах гражданско-правового характера с иными лицами должны быть предусмотрены условия о неразглашении Сотрудниками и иными лицами как охраняемой законом банковской, коммерческой или иной законодательно определенной тайны, имеющей в своем составе персональные данные, так и отдельных категорий персональных данных, не входящих в состав тайн.

5. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Технология обработки персональных данных сотрудниками включает в себя следующие процессы: получение (сбор); уточнение (обновление, изменение); систематизация и накопление; использование; хранение; уничтожение.

5.2. Персональные данные субъекта получаются, как правило, от него самого, за исключением случаев, когда их получение возможно только у третьей стороны.

5.3. Банком не осуществляется обработка персональных данных субъекта о его политических, религиозных и иных убеждениях, частной жизни, за исключением случаев, непосредственно связанных с вопросами трудовых отношений. В данных случаях, в соответствии со статьей 24 Конституции РФ, Банк вправе обрабатывать данные о частной жизни субъекта только с его письменного согласия.

5.4. Банком не осуществляется обработка персональных данных субъекта о его членстве в общественных объединениях, за исключением случаев, предусмотренных законодательством РФ.

5.5. В процессе сбора и уточнения персональных данных сотрудники обязаны:

– контролировать своевременность актуализации персональных данных;
– обеспечить полноту и достоверность обрабатываемых данных;
– обеспечить безопасное хранение полученных данных.

5.5.2. Если предоставление персональных данных является обязательным, в соответствии с Федеральным законом №152-ФЗ, Банк обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

5.6. В процессе систематизации и накопления сотрудники обязаны обеспечить полноту и достоверность информации.

5.7. В процессе использования сотрудники обязаны:

– контролировать полноту и достоверность полученных сведений;
– обеспечить безопасное хранение персональных данных.

5.8. При необходимости получения Банком персональных данных не от самого субъекта персональных данных, например, при осуществлении сделок с корпоративными клиентами, в соответствии с Федеральным законом №152-ФЗ Банк, за исключением случаев, предусмотренных законодательством Российской Федерации, до начала обработки таких персональных данных обязан предоставить этому субъекту персональных данных следующую информацию:

– наименование и адрес Банка;
– цель обработки персональных данных и ее правовое основание;
– предполагаемые пользователи персональных данных;
– установленные Федеральным законом №152-ФЗ права субъекта персональных данных;
– источник получения персональных данных.

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

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

– персональных данных получены Банком на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

– персональных данных сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

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

– предоставление субъекту персональных данных сведений, указанных в п.5.8 настоящего Положения, нарушает права и законные интересы третьих лиц.

5.10. Согласие субъекта персональных данных.

5.10.1. В соответствии с Федеральным законом №152-ФЗ субъект персональных данных принимает решение о предоставлении его персональных данных и дает Согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информативным и сознательным.

5.10.2. Согласие может быть дано субъектом персональных данных или его Представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения Согласия от Представителя субъекта персональных данных полномочия данного Представителя на дачу Согласия от имени субъекта персональных данных проверяются Банком.

5.10.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных Согласия на обработку персональных данных Банк вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона №152-ФЗ.

5.10.4. Обязанность предоставить доказательство получения Согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных выше, возлагается на Банк.

5.10.5. В определенных Федеральным законом №152-ФЗ случаях, обработка персональных данных может осуществляться только с согласия субъекта персональных данных в письменной форме. Согласие в письменной форме необходимо в случаях обработки специальных категорий персональных данных, биометрических персональных данных, трансграничной передачи персональных данных, а также в случаях принятия решения, порождающего юридические последствия в отношении субъекта персональных данных, на основании исключительно автоматизированной обработки его персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается Согласие в форме электронного документа, подписанного в соответствии с действующим законодательством Российской Федерации электронной подписью или аналогом собственноручной подписи. Форма Согласия представлена в Приложении №2 к настоящему Положению. Также Согласие может содержаться в договорах, заключаемых Банком с Клиентами (в этом случае предоставление отдельного экземпляра Согласия не требуется).

5.10.6. В случае недееспособности субъекта персональных данных Согласие на обработку его персональных данных дает законный представитель субъекта персональных данных. В случае смерти субъекта персональных данных Согласие дают наследники субъекта персональных данных, если такое Согласие не было дано субъектом персональных данных при его жизни, персональные данные могут быть получены Банком от лица, не являющегося субъектом персональных данных, при условии предоставления Банку подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона №152-ФЗ.

5.10.7. В соответствии с Федеральным законом №152-ФЗ Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя:

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

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

документа и выдавшем его органе, реквизиты документа, подтверждающего полномочия этого Представителя (при получении согласия от Представителя субъекта персональных данных);

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

- цель обработки персональных данных;

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

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

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

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

- подпись субъекта персональных данных.

5.10.8. В случае отзыва субъектом персональных данных Согласия на обработку его персональных данных Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором или иным соглашением между Банком и субъектом персональных данных либо, если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством РФ.

5.11. 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.

5.12. Банк вправе поручить обработку персональных данных другому лицу с Согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональных данных, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных.

5.13. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать Согласие субъекта персональных данных на обработку его персональных данных.

5.14. В случае, если Банк поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Банк. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед Банком.

5.15. Обработка персональных данных осуществляется на основе следующих законодательно определенных принципов:

- на законной и справедливой основе;
- ограничиваться достижением конкретных, заранее определенных и законных целей;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем должны соответствовать заявленным целям обработки, и не должны быть избыточными;
- должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;

- уничтожению либо обезличиванию персональных данных подлежат по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.16. Обработка персональных данных Сотрудников, родственников Сотрудников должна осуществляться в соответствии с действующими требованиями и нормами «Положения об обработке персональных данных сотрудников».

5.17. Обработка персональных данных клиентов и иных лиц должна осуществляться в соответствии с действующими требованиями и нормами «Положения об обработке персональных данных клиентов и иных лиц».

5.18. Учет, использование, хранение и уничтожение машинных и бумажных носителей информации, содержащих персональные данных, должен осуществляться в соответствии с «Инструкцией по работе с носителями информации, содержащими сведения конфиденциального характера в АО КБ «АГРОПРОМКРЕДИТ».

5.19. При обработке персональных данных обеспечивается конфиденциальность, т.е. созданы условия, не допускающие их распространения или предоставления третьим лицам без согласия субъекта персональных данных, за исключением случаев, определенных законодательством РФ и/или, когда персональные данные относятся к обезличенным/общедоступным.

5.20. Передача персональных данных субъектов между подразделениями Банка осуществляется только между Сотрудниками, допущенными к обработке персональных данных.

5.21. Сроки обработки и хранения персональных данных:

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

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

5.21.3. Процедура хранения персональных данных в Банке проводится в порядке, который позволяет осуществлять хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок их хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Данный порядок соответствует определенному в ч.7 ст. 5 Федерального закона №152-ФЗ принципу обработки персональных данных.

5.21.4. Сроки хранения персональных данных в Банке, в общем случае, определяются в соответствие со сроками, установленными приказом Министерства культуры РФ от 25.08.2010 №558 об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», Перечнем типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения, утвержденный приказом Министерства культуры и массовых коммуникаций Российской Федерации от 31.07.2007 №1182, Постановлением ФКЦБ РФ от 16.07.2003 №03-33/пс «Об утверждении Положения о порядке и сроках хранения документов акционерных обществ», а также иными требованиями законодательства РФ (по срокам исковой давности, по оформлению трудовых отношений и т.д.), нормативных документов федеральных органов исполнительной власти и Банка России, документов, фиксирующих договорные отношения Банка с субъектами персональных данных, и Согласий субъектов на обработку персональных данных.

5.21.5. В случае достижения цели обработки персональных данных Банк обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором между Банком и субъектом персональных данных либо, если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством РФ.

5.21.6. Уничтожение персональных данных в информационных системах, на машинных и бумажных носителях информации производится в течение тридцати дней с даты достижения цели обработки (предельного срока хранения) персональных данных.

5.21.7. В случае отсутствия возможности уничтожения в течение указанного срока, Банк осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по его поручению) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами РФ.

5.22. Обращения и запросы субъектов персональных данных в отношении обработки их персональных данных обрабатываются в соответствии с положениями «Регламента реагирования на обращения и запросы по вопросам обработки персональных данных в АО КБ «АГРОПРОМКРЕДИТ».

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

6.1. Персональные данные при их обработке без использования средств автоматизации обособляются от иной информации путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

6.2. При фиксации персональных данных на материальных носителях не допускается запись на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы. При обработке различных категорий персональных данных без использования средств автоматизации для каждой категории персональных данных используется отдельный материальный носитель.

6.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, соблюдаются следующие условия:

- типовая форма должна содержать сведения о цели обработки персональных данных, наименование и адрес Банка, 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;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных - при необходимости получения письменного согласия на обработку персональных данных;
- 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;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.4. 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, применяются меры по обеспечению раздельной обработки персональных данных.

6.5. Банк обеспечивает раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

6.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

6.7. Уточнение персональных данных при их обработке 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.

6.8. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, информируются:

- о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации;
- о категориях обрабатываемых персональных данных;
- об особенностях и правилах осуществления такой обработки.

7. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности Банка. При обработке персональных данных Банк принимает необходимые правовые, организационные и технические меры для защиты персональных данных от НСД или случайных действий с персональными данными (доступ, уничтожение, изменение, блокирование, копирование, предоставление, распространение), а также от иных неправомерных действий в отношении персональных данных. Выбор и реализация методов и способов защиты персональных данных в ИСПДн осуществляется на основании уровня защищенности персональных данных при их обработке в ИСПДн, исходя из угроз безопасности персональных данных.

7.2. Организация работ по обеспечению безопасности персональных данных осуществляется ДЭБиР Банка при непосредственном участии Руководства Банка.

7.3. Обеспечение безопасности персональных данных при их обработке, реализуется с учетом законодательных актов РФ, норм и требований Регуляторов, а также в соответствии с внутрибанковскими нормативными документами в области обеспечения информационной безопасности.

7.4. Обеспечение защищенности персональных данных достигается благодаря:

- недопущению воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
- постоянному контролю обеспечения уровня защищенности персональных данных;
- определению угроз для безопасности персональных данных при их обработке;
- применению организационных и технических мер по обеспечению безопасности персональных данных, необходимых для выполнения требований к защите персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;
- учету и контролю машинных носителей, содержащих персональные данные;
- своевременному выявлению фактов НСД и принятию мер по локализации;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлению жестких правил доступа к персональным данным, а также обеспечению регистрации и учету всех действий, совершаемых с персональными данными;
- контролю за принимаемыми мерами по обеспечению безопасности персональных данных.

7.5. Для всех ИСПДн Банка проводится определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных. Мероприятия по определению уровня защищенности проводятся в соответствии с порядком, определенным Постановление Правительства РФ от 01.11.2012 №1119, комиссией, назначаемой приказом Председателя Правления Банка. Результаты оформляются актом определения уровня защищенности персональных данных при их обработке в ИСПДн Банка. Тип угроз, актуальных для ИСПДн, определяется в соответствии с частной моделью угроз для данной ИСПДн. Форма Акта приведена в Приложении №6 к настоящему Положению.

7.6. На основании Частного Технического задания и Частной модели угроз разработан Технический проект, который предназначен для реализации комплексных мер по защите персональных данных и включает следующие подсистемы: антивирусная защита; межсетевое экранирование; управление доступом; регистрация и учет; обеспечение целостности; обнаружение вторжений; анализ защищенности.

7.7. В случае использования и хранения биометрических персональных данных вне ИСПДн, обработка таких данных может осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

7.8. Контроль исполнения организационно-технических и эксплуатационных мероприятий при обеспечении безопасности персональных данных возлагается на Управление технических средств безопасности и режима ДЭБиР Банка.

8. ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ С ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Перечень мер и комплекс мероприятий, направленных на предотвращение неправомерного использования персональных данных, включает в себя:

– выявление совершённых в процессе выполнения служебных обязанностей сотрудниками Банка действий, нарушающих требования работы с персональными данными субъектов;

– признание этих действий/бездействий в установленном порядке недействительными, предотвращение и возмещение вреда;

– привлечение виновных к ответственности.

8.2. К организационным мерам выявления и предотвращения неправомерных действий с персональными данными относятся:

– инструктаж и ознакомление с основополагающими законодательными актами РФ и внутрибанковскими документами по вопросам информационной безопасности вновь принятых сотрудников;

– периодическое информирование сотрудников о новых и действующих требованиях законодательства РФ в области защиты персональных данных, о возможных угрозах, ошибках и нарушениях, допускаемых при обработке персональных данных, а также ответственности при их совершении;

– служебное расследование фактов неправомерного обращения с персональными данными.

8.3. ИСПДн должна поддерживать журналирование действий пользователей при обработке персональных данных в системе. Технические меры выявления неправомерных действий с персональными данными реализуются путем анализа электронных журналов, на предмет выявления нарушений действующих требований работы с персональными данными.

9. ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ЗАПРЕЩАЕТСЯ

В целях обеспечения защиты обрабатываемых персональных данных в Банке и его подразделениях запрещается:

– осуществлять обработку информации, содержащую персональные данные субъекта, без обеспечения соответствующей защиты и наличия разрешения на выполнения данных операций;

– обрабатывать персональные данные в присутствии лиц, не допущенных к данной информации, при невозможности исключить акустический или визуальный доступ данных лиц к конфиденциальным сведениям в момент обработки;

– осуществлять ввод/запись персональных данных под диктовку, за исключением случаев, при которых ввод/запись происходит под диктовку субъекта персональных данных по телефону;

– озвучивать/произносить вслух персональные данные субъекта персональных данных при их обработке;

– несанкционированно подключать технические средства и инсталлировать программные продукты, непредусмотренные для использования в ИСПДн;

– изменять состав и конфигурацию программных и технических средств ИСПДн;

– несанкционированно использовать в защищаемых помещениях технические устройства любых систем связи, средств передачи информации и фото/видео/звукорегистрации;

– фиксировать на одном бумажном носителе различные персональные данные, цели обработки которых заведомо несовместимы.

10. СРЕДСТВА И МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Применяемые средства защиты информации.

10.1.1. Средства защиты информации (далее – СЗИ), применяемые в информационных системах Банка, в установленном законодательством РФ порядке, проходят процедуру оценки соответствия.

10.1.2. СЗИ, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, а также эксплуатационная и техническая документация к ним подлежат учету в соответствии с порядком, определенным в Банке.

10.1.3. До ввода в эксплуатацию все СЗИ, устанавливаемые в Банке проходят проверку готовности их использования с составлением заключения о возможности их эксплуатации (форма заключения приведена в Приложении №9 к настоящему Положению). При положительном заключении о возможности эксплуатации данные средства вводятся в эксплуатацию с составлением акта (форма акта внедрения средств защиты информации приведена в

Приложении №3 к настоящему Положению). Проверка и ввод средств защиты производится комиссией, назначенной приказом Председателем Правления Банка.

10.1.4. Установка и ввод таких средств в эксплуатацию осуществляется в соответствии с эксплуатационной и технической документацией на СЗИ.

10.1.5. Контроль соблюдения порядка и условий использования СЗИ, предусмотренных эксплуатационной и технической документацией, возлагается на Лицо ответственное за обеспечение безопасности персональных данных.

10.1.6. Сотрудники Банка, использующие СЗИ, применяемые в ИСПДн, должны быть обучены правилам работы с ними.

10.2. Организационные меры.

10.2.1. Для обеспечения безопасности персональных данных при их обработке в ИСПДн Банка применяются следующие организационные меры:

- обеспечение учета, хранения, обращения и уничтожения машинных носителей персональных данных;
- ознакомление Сотрудников с внутренними требованиями Банка по защите персональных данных;
- обеспечение контроля доступа в помещения, в которых находятся технические средства обработки персональных данных, хранятся машинные носители персональных данных;
- размещение технических средств обработки персональных данных в пределах контролируемой зоны;
- обеспечение пропускного режима на территорию Банка, охраны помещений с установленными техническими средствами обработки персональных данных.

10.3. Технические меры.

10.3.1. Для обеспечения безопасности персональных данных при их обработке в ИСПДн Банка применяются следующие технические меры:

- установление и реализация правил предоставления доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты персональных данных;
- регистрация и учет действий пользователей, совершаемых с персональными данными в ИСПДн;
- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных;
- осуществление антивирусного контроля;
- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
- применение средств межсетевого экранирования;
- централизованное управление системой защиты персональных данных.

10.4. Контроль применяемых мер защиты.

10.4.1. С целью поддержания уровня защищенности персональных данных в Банке реализована система контроля применяемых мер по защите персональных данных.

10.4.2. В ходе мероприятий по контролю осуществляется:

- проверка выполнения требований нормативных документов по защите персональных данных;
- оценка обоснованности и эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;
- систематическое проведение мониторинга действий пользователей, доведение его результатов до сведения руководства Банка, проведение разбирательств и составление заключений по фактам нарушения требований безопасности персональных данных.

10.5. Внутренний контроль принимаемых в Банке мер по обеспечению безопасности персональных данных при их обработке в ИСПДн организует и осуществляет Лицо ответственное за обеспечение безопасности персональных данных.

10.6. Для проведения внешнего контроля и аудита безопасности персональных данных Банка на договорной основе может привлекаться сторонняя организация, обладающая лицензией на деятельность по технической защите конфиденциальной информации.

11. ОРГАНИЗАЦИЯ РЕЖИМА БЕЗОПАСНОСТИ ПОМЕЩЕНИЙ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Размещение информационных систем и специального оборудования, а также организация режима обеспечения безопасности помещений, в которых ведется работа с персональными данными, обеспечивает сохранность носителей персональных данных и средств защиты информации, а также исключает возможность неконтролируемого проникновения или

пребывания в этих помещениях посторонних лиц.

11.2. Доступ в такие помещения производится на основании списка, утвержденного уполномоченным лицом Банка (форма списка приведена в Приложении №11 к настоящему Положению).

11.3. Хранение машинных носителей информации осуществляется в запираемых шкафах, исключающих несанкционированный доступ к ним.

11.4. Размещение технических средств обработки персональных данных в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность несанкционированного доступа к ним, в том числе просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

11.5. Режим охраны помещений устанавливается исходя из внутреннего трудового распорядка Банка.

11.6. Контроль соблюдения установленного режима работы в повседневной деятельности и охраны помещений возлагается на руководителей структурных подразделений.

11.7. Функции по организации пропускного режима на территорию Банка или их часть могут выполняться сторонней организацией на основании договора. Договором должен быть определен порядок пропуска лиц на территорию Банка, порядок регистрации соответствующих лиц, порядок вноса и выноса имущества, а также охраны помещений в нерабочее время.

12. ОБЯЗАННОСТЬ И ОТВЕТСТВЕННОСТЬ

12.1. В соответствии со ст. 22 Федерального закона №152-ФЗ Банк до начала обработки персональных данных уведомил уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

12.2. В соответствии с требованиями Федерального закона №152-ФЗ и Постановления Правительства РФ №1119 от 01.11.2012 г. Приказом по Банку назначены: Лицо, ответственное за организацию обработки персональных данных в Банке; Лица, ответственные за организацию обработки персональных данных (в рамках направлений деятельности); Лицо, ответственное за обеспечение безопасности персональных данных в Банке; Структурное подразделение, ответственное за организацию защиты персональных данных и Лицо, в обязанности которого входит доведение до сведения Сотрудников требований к защите персональных данных и осуществление контроля за их выполнением.

12.3. Лицо, ответственное за организацию обработки персональных данных и Лицо, ответственное за обеспечение безопасности персональных данных, получают указания непосредственно от исполнительного органа Банка и подотчетны ему.

12.4. Лицо, ответственное за обеспечение безопасности персональных данных, обязано:

- осуществлять координацию организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в информационных системах персональных данных;
- участвовать в планировании мероприятий по защите информации и осуществлению контроля их выполнения и эффективности;
- осуществлять внутренний контроль за соблюдением в Банке законодательства РФ о защите персональных данных

12.5. На Лиц, ответственных за организацию обработки персональных данных (в рамках направлений) возлагаются следующие обязанности:

- руководить работой комиссии по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных;
- осуществлять внутренний контроль за соблюдением сотрудниками Банка требований законодательства Российской Федерации при обработке персональных данных;
- доводить до сведения сотрудников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных;
- организовывать приём и обработку обращений и запросов субъектов персональных данных (их представителей) и (или) осуществлять контроль за приёмом и обработкой таких обращений и запросов.

12.6. Ознакомление Сотрудников, принимаемых на работу в Банк с внутрибанковскими нормативными документами, а также нормативными актами и законодательством Российской Федерации в области безопасности информации, в том числе защиты персональных данных, в Головном Банке (далее – ГБ) осуществляет Управление по работе с персоналом Банка, в филиалах – специалисты по работе с персоналом или лица, исполняющие обязанности по работе с персоналом. В случае необходимости дополнительного консалтинга или информационной поддержки, привлекаются сотрудники ДЭБиР (в филиалах - СЭБ) и/или сотрудники других подразделений.

12.7. В случае предоставления персональных данных третьим лицам все сведения о передаче персональных данных субъектов регистрируются в «Журнале учета передачи персональных данных» (Приложение №4 к настоящему Положению). Учет и регистрация сведений о передаче персональных данных осуществляется Ответственным лицом за организацию обработки персональных данных (в рамках направлений).

12.8. Контроль за выполнением требований настоящего Положения осуществляется ДЭБиР Банка в соответствии с «Планом внутренних мероприятий и проверок состояния защиты персональных данных» (Приложение №5 настоящего Положения).

12.9. Каждый сотрудник Банка, получающий для работы конфиденциальный документ, содержащий персональных данных субъекта, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

12.10. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами Российской Федерации и настоящим Положением.

12.11. Административная ответственность.

В соответствии со ст. 13.14 Кодекса Российской Федерации об административных правонарушениях разглашение персональных данных (за исключением случаев, если такое разглашение влечет уголовную ответственность) лицом, получившим доступ к персональным данным в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа на должностных лиц в размере от четырех до пяти тысяч рублей.

12.12. Дисциплинарная ответственность.

Неправомерное разглашение персональных данных лицом, в чьи обязанности входит соблюдение правил хранения, обработки и использования такой информации, также является основанием для привлечения этого лица к дисциплинарной ответственности. Согласно п.п. «в» п. 6 ч. 1 ст. 81 Трудового кодекса Российской Федерации, трудовой договор с Сотрудником может быть расторгнут по причине разглашения охраняемой законом тайны, ставшей известной Сотруднику в связи с исполнением им трудовых обязанностей, в том числе по причине разглашения персональных данных.

12.13. Уголовная ответственность.

В соответствии со ст. 137 Уголовного кодекса Российской Федерации незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации наказываются штрафом в сумме до двухсот тысяч рублей или в размере заработной платы либо иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев. Часть 2 указанной статьи предусматривает, что те же деяния, совершенные лицом с использованием своего служебного положения, наказываются штрафом в сумме от ста тысяч до трехсот тысяч рублей или в размере заработной платы либо иного дохода, осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев.

12.14. Материальная ответственность.

Трудовым кодексом Российской Федерации предусмотрена материальная ответственность за виновное нарушение норм, регулирующих получение, обработку и защиту персональных данных. Так, в результате незаконного распространения информации о персональных данных последнему может быть причинен моральный вред, подлежащий возмещению. В соответствии со ст. 238 Трудового кодекса Российской Федерации оператор, обрабатывающий персональные данные обязан возместить причиненный прямой действительный ущерб. Согласно ч. 2 указанной статьи под прямым действительным ущербом также понимается необходимость возмещения ущерба третьим лицам. Следовательно, если вред субъекту персональных данных был допущен по вине лица, которое было ответственно за неразглашение персональных данных оператор персональных данных может привлечь последнее к материальной ответственности за ущерб, который был нанесен субъекту персональных данных такими действиями.

Приложение № 1
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

ОБЯЗАТЕЛЬСТВО

о неразглашении персональных данных
АО КБ «АГРОПРОМКРЕДИТ»

Я, _____,
Фамилия, Имя, Отчество

с Положением о порядке обработки и защите персональных данных АО КБ «АГРОПРОМКРЕДИТ» и с другими внутрибанковскими нормативными документами, регламентирующими процессы обработки персональных данных, ознакомлен и обязуюсь не разглашать персональные данные субъектов персональных данных, ставшие мне известными в связи с исполнением моих должностных обязанностей, информировать руководителя и ответственных сотрудников, в соответствии с Положением о порядке обработки и защите персональных данных АО КБ «АГРОПРОМКРЕДИТ», об утрате документов, о фактах нарушения порядка обращения с ними, о попытках несанкционированного доступа к персональным данным и использовать эти данные лишь в целях, для которых они сообщены.

Об ответственности за разглашение персональных данных сотрудников предупрежден(а). Мне известно, что нарушение этих требований может повлечь уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

_____ _____ _____
должность подпись Фамилия, Имя, Отчество

« ___ » _____ 20 __ г.

Экземпляр Обязательства получил(а):
Сотрудник _____ _____
подпись Фамилия, Имя, Отчество

Приложение № 2
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

СОГЛАСИЕ

субъекта персональных данных на обработку его персональных данных
и информирование субъекта персональных данных

*Я,*_____

Ф.И.О. физического лица - заявителя

_____

паспортные данные физического лица – заявителя, кем и когда выдан

_____

адрес регистрации физического лица – заявителя

Настоящим выражаю АО КБ «АГРОПРОМКРЕДИТ» (включая структурные подразделения Банка) расположенному по адресу: Московская область, г. Лыткарино, 5 микрорайон, квартал 2, дом 13 (далее – Банк) свое Согласие на обработку Банком всех моих персональных данных.

При этом под персональными данными понимаются относящиеся ко мне сведения и информация на бумажных и/или электронных носителях, которые были или будут переданы в Банк лично мной и/или доверенным лицом, либо поступили (поступят в будущем) в Банк: фамилия, имя, отчество; дата, месяц, год рождения; место рождения; адрес; паспортные данные (серия, номер, кем и когда выдан); семейное, социальное, имущественное положение; контактная информация (телефон, e-mail); профессия, образование, доходы и любые иные сведения и информация, относящаяся к моей личности, предоставленная Банку (далее – Персональные данные).

Настоящее Согласие дается Банку на обработку персональных данных для следующих целей:

– принятия Банком решения о заключении кредитных договоров, договоров по оказанию банковских услуг и их дальнейшего исполнения;

– информирования Банком Клиента о банковских услугах и продуктах Банка и его партнеров;

– продвижения товаров, работ, услуг Банка и его партнеров на рынке, в т.ч. путем осуществления прямых контактов с Клиента с помощью средств связи (в т.ч. телефон, Интернет, почта и др.);

– проведения маркетинговых исследований рынка банковских услуг;

– защиты жизни и имущества Клиента в Банке (фото/видеорегистрация);

– осуществления Банком возложенных на него функций в соответствии с законодательством РФ, принятыми нормативными актами Банка России (в т.ч. Налоговым кодексом РФ, Трудовым кодексом РФ, федеральными законами «О банках и банковской деятельности», «О кредитных историях», «Об исполнительном производстве», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «О страховании вкладов физических лиц в банках Российской Федерации», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных» и др.).

Настоящее Согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая, но, не ограничиваясь, сбор, систематизацию, накопление, хранение, уточнение, (обновление, изменение), использование, распространение (в случаях, прямо предусмотренных действующим законодательством РФ с соблюдением банковской тайны), передача обезличивание, блокирование, уничтожение персональных данных, а также осуществление любых иных действий с моими персональными данными с учетом действующего законодательства.

/_____/ Подпись_____

Я подтверждаю, что ознакомлен(а) с перечнем операций с моими персональными данными, а также правилами обработки персональных данных Банком, осуществляемой как с использованием средств автоматизации (автоматизированная обработка), так и без использования таких средств (неавтоматизированная обработка). Мне также разъяснен порядок принятия решений на основании исключительно автоматизированной обработки моих персональных данных и возможных юридических последствий такого решения. В целях исполнения договоров, заключенных между мной и Банком, в том числе даю согласие на обработку своих персональных данных, при которой будут приниматься решения на основании исключительно автоматизированной обработки моих персональных данных.

Разрешаю запрашивать в Бюро кредитных историй и направлять в Бюро кредитных историй информацию о моей кредитной истории.

В целях уступки долговых обязательств полностью или частично настоящее Согласие разрешает направленную передачу персональных данных новому владельцу долговых обязательств в соответствии с действующим законодательством Российской Федерации. Данное Согласие не является согласием на обработку третьей стороне. Новый владелец долговых обязательств самостоятельно отвечает за соблюдение требований действующего законодательства Российской Федерации по обработке персональных данных.

Настоящее Согласие действует до истечения 5 (пяти) лет с момента прекращения действия последнего из договоров, заключенных между мной и Банком. По истечении указанного срока действие Согласия считается продленным на каждые следующие 5 (пять) лет при условии отсутствия у Банка сведений о его отзыве.

Настоящим я уведомлен, что отзыв данного Согласия может быть осуществлен мной при условии письменного уведомления Банка за 2 (два) месяца до момента отзыва Согласия. Данный срок исчисляется со дня следующего за днем получения Банком уведомления об отзыве Согласия.

Настоящим выражаю свое согласие на получение мной рекламной информации о продуктах и услугах (как новых, так и действующих) Банка и партнеров Банка, а также на получение любой другой информации.

Настоящим выражаю согласие на получение вышеуказанной рекламной информации любым доступным Банку способом, в том числе по сетям электросвязи посредством использования телефонной, факсимильной, подвижной радиотелефонной связи, сети Интернет, факс, СМС–сообщений.

Контактная информация:

Тел. _____, Моб. Тел. _____, E-mail_____

Почтовый адрес _____

Иная информация _____

Дата «___» _____ 20____ г.

Подпись_____ /_____/

Приложение № 3
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

Утверждаю
Председатель Правления
АО КБ «АГРОПРОМКРЕДИТ»
В.А. Корнев

«___» _____ 20___г.

Акт
внедрения средств защиты информации в

_____
наименование информационной системы

Комиссия в составе:

Председатель: _____
_____
Члены комиссии: _____
_____
_____

рассмотрев исходные данные на установленное и настроенное:

_____
_____
наименование подразделения или подрядчика, установившего СЗИ

средство защиты _____,

РЕШИЛА:
считать средство защиты

_____
наименование информационной системы

_____успешно внедренным в ИСПДн

Председатель Комиссии _____ _____
(личная подпись) (фамилия, имя, отчество)

Члены Комиссии _____ _____
(личная подпись) (фамилия, имя, отчество)

_____ _____
(личная подпись) (фамилия, имя, отчество)

_____ _____
(личная подпись) (фамилия, имя, отчество)

Приложение № 4
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

ЖУРНАЛ

учета передачи персональных данных
АО КБ «АГРОПРОМКРЕДИТ»

№	Вид носителя	Учетный номер (в случае наличия)	Ответственное лицо	Подпись ответственного лица	Куда передаются персональные данные	Основание передачи	Передаваемые данные	Дата передачи	Сведенья о возврате или удалении

Приложение № 5
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

ПЛАН

внутренних мероприятий и проверок соблюдения требований к организации обработки и защите персональных данных в АО КБ «АГРОПРОМКРЕДИТ»

№ п/п	Наименование мероприятия	Периодичность выполнения	Ответственные за выполнение
1.	Пересмотр Моделей угроз безопасности	При изменении в законодательстве или типов угроз	Управление технических средств безопасности и режима
2.	Проверка актуальности внутрибанковских нормативных документов, регламентирующих обеспечение безопасности персональных данных	Не реже одного раза в год	Управление технических средств безопасности и режима
3.	Проверка актуальности внутрибанковских нормативных документов, регламентирующих организацию обработки персональных данных	Не реже одного раза в год	Лица, ответственные за организацию обработки персональных данных (в рамках направлений)
4.	Сверка действующей редакции Списка лиц, допущенных к обработке персональных данных	Не реже одного раза в квартал	Управление технических средств безопасности и режима
5.	Проверка качества знаний сотрудников в вопросах обеспечения безопасности персональных данных и защиты информации	Раз в год	Управление по работе с персоналом
6.	Контроль за использованием средств защиты информации и обеспечением безопасности персональных данных	Регулярно	Управление технических средств безопасности и режима
7.	Контроль за соблюдением требований к организации обработки персональных данных	Регулярно	Лица, ответственные за организацию обработки персональных данных (в рамках направлений)
8.	Проверка Списка лиц, допущенных к обработке персональных данных	Ежеквартально	Управление технических средств безопасности и режима
9.	Контроль содержания типовых форм документов, предполагающих и/или допускающих содержание персональных данных	Регулярно	Юридический департамент и Лица, ответственные за организацию обработки персональных данных (в рамках направлений)

Приложение № 6
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

УТВЕРЖДАЮ
Председатель Правления
АО КБ «АГРОПРОМКРЕДИТ»

_____
«_____» _____ _____г.

АКТ № ___
определения уровня защищенности персональных данных при их обработке
в информационной системе персональных данных
«_____»

В соответствии с постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» Комиссия, назначенная Приказом Председателя Правления АО КБ «АГРОПРОМКРЕДИТ» от ____ . ____ . _____ № _____ «О назначении Комиссии по организации обработки персональных данных», в составе:

Председатель Комиссии: _____
(должность, фамилия, имя, отчество)

Члены Комиссии: _____
_____
_____
(должность, фамилия, имя, отчество)

рассмотрев следующие исходные данные на информационную систему персональных данных (ИСПДн) «_____»:

1. Категория обрабатываемых в ИСПДн персональных данных.
2. Субъекты, персональные данные которых обрабатываются в ИСПДн.
3. Объем обрабатываемых в ИСПДн персональных данных.
4. Тип актуальных угроз безопасности персональных данных.

РЕШИЛА:

В соответствии с п.12 Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» при обработке персональных данных в ИСПДн «_____» присвоить ___ уровень защищенности персональных данных.

Председатель Комиссии _____ (личная подпись) _____ (фамилия, имя, отчество)

Члены Комиссии _____ (личная подпись) _____ (фамилия, имя, отчество)

_____ (личная подпись) _____ (фамилия, имя, отчество)

_____ (личная подпись) _____ (фамилия, имя, отчество)

Приложение № 7
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

ФОРМЫ ОТЧЕТНОСТИ

при изменениях Штатного расписания, увольнении, приеме и переводе сотрудника

I. Ввести в Штатное расписание:

_____ *(ГБ/филиал)*		
№ п/п	**Подразделение**	**Должность**
1.		

II. Вывести из Штатного расписания:

_____ *(ГБ/филиал)*		
№ п/п	**Подразделение**	**Должность**
1.		

III. Увольнение сотрудника

Наименование (ГБ/филиал)	Ф.И.О. сотрудника	Должность	Наименование структурного подразделения	Дата увольнения	Дата прекращения доступа к внутрибанковским ресурсам

Декретный отпуск

Наименование (ГБ/филиал)	Ф.И.О. сотрудника	Наименование структурного подразделения	Дата ухода в декретный отпуск	Дата выхода из декретного отпуска

IV. Прием и перевод сотрудника

При приеме:

Наименование (ГБ/филиал)	Ф.И.О. сотрудника	Должность	Наименование структурного подразделения	Дата приема на работу

При переводе:

Наименование (ГБ/филиал)	Ф.И.О. сотрудника	Должность (старая/новая)	Наименование структурного подразделения (старое/новое)	Дата перевода

Приложение № 8
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

Нормативные ссылки

Конституция Российской Федерации; Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»; Гражданский кодекс Российской Федерации; Налоговый кодекс Российской Федерации; Трудовой кодекс Российской Федерации; Федеральный закон от 10.07.2002 №86-ФЗ «О Центральном банке Российской Федерации (Банке России)»; Федеральный закон от 02.12.1990 №395-1 «О банках и банковской деятельности»; Федеральный закон от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»; Федеральный закон «О кредитных историях» от 30.12.2004 №218-ФЗ; Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 23.12.2003 №177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации»; Федеральный закон «О коммерческой тайне» от 29.07.2004 №98-ФЗ; Федеральный закон от 26.12.1995 №208-ФЗ «Об акционерных обществах»; Постановление Правительства РФ от 15.09.2008 №687; Постановление Правительства Российской Федерации от 01.11.2012 №1119; Приказ ФСТЭК России от 11.02.2013 №17; Комплекс стандартов Банка России СТО БР ИББС; Устав Банка и другие, действующие законодательные и нормативные акты, в том числе Регуляторов.

.

Приложение № 9
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

ЗАКЛЮЧЕНИЕ № ___

о возможности эксплуатации средства защиты информации

_____
(наименование)

В соответствии с Постановлением Правительства Российской Федерации от 10.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» комиссией, назначенной приказом Председателя Правления АО КБ «АГРОПРОМКРЕДИТ» от __.__.____ № _____ «О создании комиссии по защите персональных данных», в составе:

Председатель Комиссии: _____
(должность, фамилия, имя, отчество)

Члены Комиссии: _____

_____

_____
(должность, фамилия, имя, отчество)

проведена установка, настройка и проверка готовности

_____
(наименование средства защиты информации)

Прикладное программное обеспечение

_____
(наименование программного обеспечения, место установки)

Информация о настройках средств защиты информации

_____
(наименование документа, по которому проводилась настройка средства защиты информации)

Выполнение требований по сертификации средства защиты информации

_____

_____

_____

_____

_____

_____

(реквизиты сертификата на средство защиты информации/не проводилась)

Вывод о возможности эксплуатации: установленное средство защиты информации

_____

(наименование)

готово к использованию в информационной системе персональных данных «_____»

(название ИСПДн)

в качестве

_____

(назначение средства защиты информации)

Председатель Комиссии

_____ _____

(личная подпись) (фамилия, имя, отчество)

Члены Комиссии

_____ _____

(личная подпись) (фамилия, имя, отчество)

_____ _____

(личная подпись) (фамилия, имя, отчество)

_____ _____

(личная подпись) (фамилия, имя, отчество)

Приложение № 10
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

ЗАКЛЮЧЕНИЕ №____
по факту несоблюдения требований безопасности персональных данных
(условий хранения носителей, использования средств защиты информации)

Комиссия, назначенная приказом Председателя Правления АО КБ «АГРОПРОМКРЕДИТ» от __.__.____ № _____ «О создании комиссии по защите персональных данных», в составе:

Председатель комиссии: _____
(должность, фамилия, имя, отчество)

Члены комиссии: _____
_____
_____
(должность, фамилия, имя, отчество)

составила настоящее заключение по факту несоблюдения условий хранения носителей персональных данных (использования средств защиты информации) Сотрудником

_____
(наименование структурного подразделения, фамилия, имя и отчество)

Комиссией установлено, что

_____
_____
_____
_____
(описание инцидента нарушения безопасности персональных данных)

Вывод: комиссия считает, что вышеперечисленные нарушения стали следствием

_____
_____
_____
_____
(причины нарушения, предложения о привлечении виновного к ответственности)

Председатель комиссии _____ _____
(личная подпись) (фамилия, имя, отчество)

Члены комиссии _____ _____
(личная подпись) (фамилия, имя, отчество)

_____ _____
(личная подпись) (фамилия, имя, отчество)

_____ _____
(личная подпись) (фамилия, имя, отчество)

Приложение № 11
к «Положению о порядке обработки и
защите персональных данных в
АО КБ «АГРОПРОМКРЕДИТ»

СПИСОК
помещений, в которых допускается обработка персональных данных

№ п/п	Наименование, номер помещения	Должностные лица, имеющие право самостоятельного доступа в помещение
1.		
2.		
3.		