Приложение 2
к приказу № 7 от « 05 » марта 2015 года

«УТВЕРЖДАЮ»

Председатель правления
КПК «Регион-Финанс»
_____ В.В.Дзюба

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
В КПК «РЕГИОН-ФИНАНС»

г. Благовещенск, 2015 г.

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ ДОКУМЕНТА

1.1. В настоящем Положении об обработке персональных данных (далее – Положение) установлены требования по организации и непосредственному функционированию процессов обработки персональных данных (далее - ПДн) в КПК «Регион-Финанс» в соответствии с требованиями нормативных правовых актов РФ в области обработки и защиты ПДн.

1.2. Требования настоящего Положения распространяются на структурные подразделения КПК «Регион-Финанс» и отдельных должностных лиц, принимающих участие в процессах обработки ПДн в КПК «Регион-Финанс».

1.3. Требования настоящего Положения распространяются на все процессы обработки ПДн в КПК «Регион-Финанс», независимо от формы представления ПДн.

2. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Термины и определения

В настоящем Положении использованы следующие термины и определения:

2.1.1. **Безопасность персональных данных** - Состояние защищенности ПДн от неправомерных действий, характеризуемое способностью пользователей, технических средств и информационных систем обеспечить конфиденциальность, целостность и доступность ПДн при их обработке, независимо от формы их представления.

2.1.2. **Внутренняя типовая форма** - Документ, состав данных и порядок обработки которого не установлен законодательством РФ, и использующийся во внутренних бизнес-процессах КПК «Регион-Финанс».

2.1.3. **Доступ к информации** - Возможность получения и использования информации.

2.1.4. **Доступность персональных данных** - Возможность беспрепятственного получения санкционированного доступа к персональным данным лицами, имеющими право на такой доступ.

2.1.5. **Защита информации** - Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

2.1.6. **Информационная система персональных данных** - Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.1.7. **Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2.1.8. **Инцидент безопасности персональных данных** - любое непредвиденное или нежелательное событие, которое может нарушить безопасность персональных данных, что может повлечь за собой нарушение деятельности КПК «Регион-Финанс».

2.1.9. **Конфиденциальность персональных данных** - Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта ПДн или иного законного основания.

2.1.10. **Несанкционированный доступ (несанкционированные действия)** - Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.

2.1.11. **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.

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

2.1.13. **Пользователь персональных данных** - Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты такой обработки.

2.1.14. **Процесс обработки персональных данных** - Бизнес-процесс КПК «Регион-Финанс», в рамках которого осуществляется обработка персональных данных.

2.1.15. **Средство вычислительной техники** - Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

2.1.16. **Средство защиты информации** - Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.1.17. **Угрозы безопасности персональных данных** - Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

2.1.18. **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.

2.1.19. **Целостность персональных данных** - Способность средства вычислительной техники или информационной системы обеспечивать неизменность персональных данных в условиях случайного и/или преднамеренного их искажения (разрушения).

2.2. Используемые сокращения

В настоящем Положении использованы сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

Сокращение	Описание
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
РФ	Российская Федерация
СЗПДн	Система защиты персональных данных
ФСБ России	Федеральная служба безопасности России

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Настоящее Положение определяет:

- принципы обработки персональных данных;
- виды обрабатываемых персональных данных;
- жизненный цикл информационных систем персональных данных;
- состав системы защиты персональных данных;
- правила обработки ПДн;
- требования по обучению персонала в области обработки ПДн;
- требования по организации доступа к персональным данным;
- требования к взаимодействию с субъектами ПДн и органами власти;
- требования к составу и содержанию документов КПК «Регион-Финанс», регламентирующих защиту и работу с ПДн.

3.2. Настоящее Положение разработано в соответствии со следующими нормативными правовыми документами:

- Конституция Российской Федерации.
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
- 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».
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- 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».
- Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 31.12. 2013 г. № 151/786/46.
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 15.02.2008 г.).
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 14.02.2008 г.).

3.3. При работе с ПДн, во всех случаях, не урегулированных внутренними нормативными документами КПК «Регион-Финанс», необходимо руководствоваться действующим законодательством РФ.

3.4. Настоящее Положение должно быть доведено до всех работников КПК «Регион-Финанс» под роспись. Подпись работника на листе ознакомления означает его согласие со всеми требованиями, указанными в настоящем Положении.

4. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В соответствии с п. 13.1 обработка ПДн в КПК «Регион-Финанс» должна осуществляться в соответствии со следующими принципами:

4.1.1. Обработка ПДн должна осуществляться на законной и справедливой основе.

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

4.1.3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.4. Обработке подлежат только ПДн, которые отвечают целям их обработки.

4.1.5. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

4.1.6. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Необходимо принимать меры по удалению или уточнению неполных или неточных данных.

4.1.7. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.1.8. Не допускается использовать ПДн в целях причинения имущественного и/или морального вреда субъектам ПДн, затруднения реализации их прав и свобод.

4.1.9. Все работники должны быть ознакомлены под подпись с документами КПК «Регион-Финанс», устанавливающими порядок обработки их ПДн, а также их правами и обязанностями в этой области, в соответствии с действующими нормативными документами.

4.2. В КПК «Регион-Финанс» должен проводиться регулярный анализ соответствия процессов обработки ПДн указанным выше принципам. Данный анализ проводится в случае:

- создания новых или внесения изменений в существующие процессы обработки ПДн;
- создания новых или внесения изменений в существующие ИСПДн;
- изменения нормативной базы затрагивающей принципы и(или) процессы обработки ПДн в КПК «Регион-Финанс»;
- проведения внутренних контрольных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

5. ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Отнесение сведений, обрабатываемых в КПК «Регион-Финанс», к категории ПДн представляет собой процесс обоснованного установления (документального оформления и утверждения руководством КПК «Регион-Финанс») критериев их выделения из всей совокупности обрабатываемых сведений.

5.2. В качестве таких критериев в отношении ПДн в КПК «Регион-Финанс» разрабатывается и утверждается перечень персональных данных (далее - Перечень ПДн). В Перечне ПДн закрепляются категории субъектов ПДн, группы и детальный состав ПДн, цели и правовые основания обработки для каждой из групп и категорий субъектов ПДн.

5.3. В КПК «Регион-Финанс» не допускается обработка ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и состояния здоровья, интимной жизни.

5.4. В КПК «Регион-Финанс» не осуществляется обработка данных о судимости.

5.5. В КПК «Регион-Финанс» не осуществляется обработка биометрических ПДн (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

6. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Комплексы баз данных, средства вычислительной техники, технических средств обработки объединяются в информационные системы персональных данных (далее – ИСПДН). При этом в одну ИСПДн может входить любое количество компонентов.

6.2. Для каждой ИСПДн КПК «Регион-Финанс» в обязательном порядке должны быть разработаны следующие документы:

- модель угроз безопасности ПДн при их обработке в ИСПДн;
- модель нарушителя в ИСПДн (может включаться в Модель угроз безопасности ПДн в ИСПДн).
- акт классификации ИСПДн.

6.3. Жизненный цикл ИСПДн КПК «Регион-Финанс» состоит из следующих стадий:

- проектирование;
- создание;
- эксплуатация;
- модернизация;
- вывод из эксплуатации.

6.4. Порядок проведения необходимых мероприятий в рамках жизненного цикла ИСПДн описан в документе «Регламент обеспечения безопасности персональных данных».

7. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. С целью выполнения требований законодательства РФ в сфере ПДн, КПК «Регион-Финанс» считает важнейшей задачей обеспечение конфиденциальности, целостности и доступности ПДн при их обработке в КПК «Регион-Финанс». Для решения данной задачи в КПК «Регион-Финанс» введена, функционирует и проходит периодический пересмотр (контроль) Система защиты персональных данных (далее – СЗПДн), которая состоит из следующих компонентов:

- организационная структура (участники обработки и ответственные лица);
- организационно-распорядительная документация;
- средства обработки ПДн;
- меры и средства обеспечения безопасности ПДн.

7.2. СЗПДн КПК «Регион-Финанс» основана на следующих принципах:

- вовлеченности руководства – деятельность по обеспечению безопасности ПДн инициирована и контролируется руководством КПК «Регион-Финанс»;
- соответствия мер и средств защиты актуальным угрозам безопасности ПДн;
- соответствия мер и средств защиты требованиям нормативных документов РФ в области обработки и обеспечения безопасности ПДн;
- комплексности - с целью обеспечения безопасности ПДн в КПК «Регион-Финанс» используется совокупность организационных и технических мер;
- патентной чистоты - средства защиты информации, входящие в состав СЗПДн КПК «Регион-Финанс», отвечают требованиям по обеспечению патентной чистоты согласно действующим нормативным документам РФ. Используемое общесистемное, специальное и прикладное программное обеспечение имеет соответствующие лицензии производителей;
- удобства персонала - при построении и модернизации СЗПДн в КПК «Регион-Финанс» учитываются и по возможности сводятся к минимуму возможные затруднения персонала в работе со средствами защиты и при выполнении основных процедур обеспечения безопасности ПДн;
- законности организационных и технических мер по обеспечению безопасности ПДн;
- непрерывности повышения уровня знаний работников КПК «Регион-Финанс» в сфере обеспечения безопасности ПДн;
- стремления к постоянному совершенствованию СЗПДн.

7.3. В соответствии с принципами обработки ПДн в КПК «Регион-Финанс» определены правила обработки ПДн (см. раздел 9 данного Положения), а также методы и способы обеспечения безопасности ПДн. Конкретные методы и способы обеспечения безопасности ПДн, а также порядок их реализации описаны в документах:

- «Регламент обеспечения безопасности персональных данных».
- «Инструкция работника по правилам обработки персональных данных».

8. ОРГАНИЗАЦИОННАЯ СТРУКТУРА КПК «РЕГИОН-ФИНАНС» В СФЕРЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. С целью организации и контроля обработки и обеспечения безопасности ПДн, в КПК «Регион-Финанс» вводятся следующие ответственные лица, которые составляют основу организационной структуры КПК «Регион-Финанс» в сфере обработки ПДн:

- ответственный за организацию обработки ПДн;
- ответственный за обеспечение безопасности ПДн:
- руководитель структурного подразделения;
- пользователь ПДн;

8.2. Возложение обязанностей по осуществлению функций указанных ответственных лиц утверждаются приказом руководителя КПК «Регион-Финанс».

8.3. Функции указанных ответственных лиц приведены в Таблице 2. При распределении ответственности за мероприятия/функции в таблице используются следующие сокращения степени участия в выполнении функций:

- «О» - организация и контроль;
- «И» - исполнение;
- «С» - согласование;
- «сИ» - соисполнение.

Таблица 2. Распределение ответственности за выполнение мероприятий в области обработки и защиты ПДн

№ п/п	Мероприятия	Ответственный за организацию обработки ПДн	Ответственный за обеспечение безопасности ПДн	Руководитель структурного подразделения	Пользователь ПДн
1	***Взаимодействие с персоналом КПК «Регион-Финанс»***				
1.1	Доведение до работников КПК «Регион-Финанс» положений законодательства РФ требований внутренней документации КПК «Регион-Финанс» в области ПДн	О, И	сИ	сИ	-
1.2	Предоставление консультаций и рекомендаций Пользователям ПДн по вопросам обработки и обеспечения безопасности ПДн	-	О,И	сИ	-
1.3	Инструктаж работников по правилам обработки ПДн	-	О, И	сИ	-
2	***Взаимодействие с субъектами ПДн и органами власти***				
2.1	Взаимодействие с субъектами ПДн или их представителями (обработка запросов/обращений, уведомление субъектов, сбор согласий на обработку ПДн)	О	-	И	-
2.2	Взаимодействие с регулирующими органами (Роскомнадзор, ФСТЭК России, ФСБ России) и иными органами власти	О, И	сИ	-	-
3	***Создание ИСПДн***				
3.1	Определение ключевых сведений об ИСПДн	О, И	сИ	сИ	-
3.2	Правовая оценка возможности создания (модернизации) ИСПДн	-	О, И	сИ	-
4	***Мониторинг и планирование***				
4.1	Мониторинг изменений законодательства РФ в области ПДн	О, И	сИ	-	-
4.2	Мониторинг СЗПДн	-	О, И	сИ	-
4.3	Планирование мероприятий по обеспечению безопасности СЗПДн (в т. ч. пересмотр СЗПДн)	-	О, И	-	-
5	***Эксплуатация СЗПДн***				

№ п/п	Мероприятия	Ответственный за организацию обработки ПДн	Ответственный за обеспечение безопасности ПДн	Руководитель структурного подразделения	Пользователь ПДн
5.1	Поддержание работоспособности компонентов СЗПДн	-	О,И	сИ	-
5.2	Управление доступом работников к ПДн	-	И	О	-
5.3	Управление доступом третьих сторон к ПДн	О, И	-	-	-
5.4	Поручение обработки ПДн	О, И	-	-	-
5.5	Учет и уничтожение машинных носителей ПДн	-	О,И	-	-
5.6	Хранение бумажных и машинных носителей ПДн	-	-	О	И
5.7	Уничтожение бумажных носителей ПДн в рабочем порядке	-	-	О	И
5.8	Централизованное уничтожение бумажных носителей ПДн	-	О	-	-
5.9	Контроль доступа на территорию	-	О	-	-
5.10	Контроль доступа в помещения с оборудованием ИСПДн	-	О	-	-
5.11	Контроль доступа к техническим средствам ИС	-	О,И	сИ	-
5.12	Контроль перемещений физических компонентов ИСПДн	-	О,И	-	-
5.13	Резервирование ПДн	-	О,И	-	-
5.14	Расследование инцидентов безопасности ПДн	-	О,И	сИ	-
5.15	Внутренние контрольные мероприятия и корректирующие действия по их результатам	-	О	-	-

9. ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Политика в отношении обработки персональных данных

9.1.1. В целях обеспечения неограниченного доступа к документу, определяющему политику КПК «Регион-Финанс» в отношении обработки ПДн и к сведениям о реализуемых требованиях к защите ПДн, в КПК «Регион-Финанс» разработан документ «Политика в области обработки и обеспечения безопасности персональных данных» (далее –Политика).

9.1.2. Политика разрабатывается на основе сведений, указанных в данном Положении, и в частности содержит:

- принципы обработки ПДн;
- категории субъектов ПДн и основные группы обрабатываемых ПДн;
- правовые основания и цели обработки ПДн;
- основные правила обработки ПДн;
- круг лиц, которым могут передаваться ПДн;
- реализуемые требования по обеспечению безопасности ПДн.

9.1.3. Открытая Политика размещена на официальном веб-сайте КПК «Регион-Финанс» и подлежит обязательному пересмотру при внесении изменений в данное Положение.

9.2. Сбор персональных данных

9.2.1. КПК «Регион-Финанс» получает ПДн из следующих источников:

- непосредственно от субъекта ПДн;
- от третьей стороны, в целях исполнения договорных обязательств или исполнения требований нормативных документов РФ;
- от другого субъекта ПДн, в целях реализации его законных прав.

9.2.2. Если предоставление ПДн является обязательным в соответствии с федеральным законом и субъект ПДн отказывается предоставить его ПДн, необходимо разъяснить субъекту ПДн юридические последствия такого отказа.

9.2.3. При сборе ПДн субъекту ПДн по его просьбе необходимо предоставить следующую информацию:

- подтверждение факта обработки ПДн;
- правовые основания и цели обработки ПДн;
- применяемые в КПК «Регион-Финанс» способы обработки ПДн;
- наименование и фактический адрес КПК «Регион-Финанс», сведения о лицах (за исключением работников КПК «Регион-Финанс»), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению КПК «Регион-Финанс», если обработка поручена или будет поручена такому лицу.

9.2.4. Общие сведения по указанным выше пунктам содержатся в Политике. Если субъект ПДн по какой-либо причине не может получить доступ к Политике, либо указанных в ней сведений недостаточно для удовлетворения просьбы субъекта ПДн, то предоставление указанных сведений осуществляется в порядке, описанном в документе «Регламент взаимодействия с субъектами персональных данных».

9.2.5. Если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн необходимо предоставить субъекту ПДн следующую информацию:

- наименование КПК «Регион-Финанс»;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- права субъекта ПДн, установленные в п. 13.1.1;
- источник получения ПДн.

9.2.5. Указанная информация может не предоставляться в следующих случаях:

- субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- ПДн получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- предоставление субъекту ПДн указанных сведений нарушает права и законные интересы третьих лиц.

9.2.6. Порядок и форма предоставления указанной в данном пункте информации описаны в документе «Регламент взаимодействия с субъектами персональных данных».

9.3. Хранение и учет персональных данных

9.3.1. В КПК «Регион-Финанс» должно быть обеспечено раздельное хранение ПДн при разных целях обработки и не допускается на одном бумажном носителе фиксация ПДн, цели обработки которых заведомо несовместимы.

9.3.2. В КПК «Регион-Финанс» должно быть по возможности обеспечено раздельное хранение ПДн, собранных с разными целями обработки.

9.3.3. Хранение ПДн в КПК «Регион-Финанс» должно осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки и требования нормативных документов РФ, связанных с хранением документов, после чего данные могут быть обезличены (при необходимости).

9.3.4. Порядок учета и хранения носителей ПДн определен в документе «Регламент обеспечения безопасности персональных данных».

9.4. Использование персональных данных

9.4.1. В КПК «Регион-Финанс» запрещено принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

9.5. Трансграничная передача

9.5.1. В КПК «Регион-Финанс» не осуществляется трансграничная передача персональных данных (передача персональных данных на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

9.6. Блокирование персональных данных

9.6.1. КПК «Регион-Финанс» блокирует обрабатываемые ПДн при выявлении недостоверности обрабатываемых ПДн или неправомерных действий в отношении субъекта в следующих случаях:

- по требованию субъекта ПДн (порядок описан в документе «Регламент взаимодействия с субъектами персональных данных»);
- по требованию уполномоченного органа по защите прав субъектов ПДн;
- по результатам внутренних контрольных мероприятий (порядок описан в документе «Регламент обеспечения безопасности персональных данных»).

9.7. Уничтожение персональных данных

9.7.1. КПК «Регион-Финанс» уничтожает персональные данные (в соответствии с действующим законодательством) в случае:

- достижения целей обработки ПДн или утраты необходимости в их достижении;

- получения соответствующего запроса от субъекта ПДн, при условии, что данный запрос не противоречит требованиям законодательства РФ;

- отзыва согласия субъекта на обработку его ПДн (если отзыв согласия влечет за собой уничтожение ПДн);

- получения соответствующего предписания от уполномоченного органа по защите прав субъектов

9.7.2. Порядок уничтожения ПДн описан в документе «Регламент обеспечения безопасности ПДн».

9.7.3. КПК «Регион-Финанс» может заключать договоры с третьими сторонами на оказание услуг по уничтожению материальных носителей. При этом КПК «Регион-Финанс» и третья сторона соблюдают все правила для обеспечения конфиденциальности уничтожаемых данных.

9.8. Особенности неавтоматизированной обработки персональных данных

9.8.1. При использовании внутренних типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны выполняться следующие условия:

- в типовые формы или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) включаются сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес КПК «Регион-Финанс», фамилия, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых в КПК «Регион-Финанс» способов обработки ПДн;

- в случае необходимости получения письменного согласия на обработку ПДн, в типовую форму включается поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации;

- типовая форма составляется таким образом, чтобы каждый из субъектов ПДн, чьи ПДн содержатся в документе, имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн;

- в типовой форме исключается объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

9.8.2. При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию КПК «Регион-Финанс» или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) оформляется приказом, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию КПК «Регион-Финанс» без подтверждения подлинности ПДн, сообщенных субъектом ПДн;

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

- ПДн каждого субъекта могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию КПК «Регион-Финанс».

10. ОБУЧЕНИЕ ПЕРСОНАЛА ПРАВИЛАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. В КПК «Регион-Финанс» все работники, участвующие в обработке ПДн, в обязательном порядке должны проходить внутренний инструктаж по следующим направлениям:

- общие вопросы обеспечения информационной безопасности в КПК «Регион-Финанс»;
- правила обработки ПДн;
- правила использования средств защиты информации, входящих в состав СЗПДн КПК «Регион-Финанс»;
- ответственность за нарушение правил обработки и обеспечения безопасности ПДн;
- новые работники в обязательном порядке проходят вводный инструктаж по указанным направлениям.

10.2. Ответственным за организацию проведения инструктажа работников КПК «Регион-Финанс», участвующих в обработке и обеспечении безопасности ПДн, является Ответственный за обеспечение безопасности ПДн.

11. УПРАВЛЕНИЕ ДОСТУПОМ К ПЕРСОНАЛЬНЫМ ДАННЫМ

11.1. Управление доступом работников к персональным данным.

11.1.1. Для определения перечня работников КПК «Регион-Финанс», допущенных к работе с ПДн, разрабатывается и утверждается перечень подразделений и лиц, допущенных к работе с ПДн, в котором указываются структурные подразделения, должности, отдельные лица (при необходимости) и группы ПДн, к работе с которыми они допущены.

11.1.2. Работник допускается к обработке ПДн только после:

- ознакомления с требованиями настоящего Положения и иными организационно-распорядительными документами СЗПДн, выполнение требований которых обязательно для соответствующих работников;
- прохождения инструктажа по правилам обработки и обеспечения безопасности ПДн;
- ознакомления с видами ответственности за нарушение установленных в КПК «Регион-Финанс» правил обработки и обеспечения безопасности ПДн.

11.1.3. При получении доступа к ПДн, работник становится Пользователем ПДн.

11.1.4. Порядок предоставления работникам доступа к обработке ПДн закреплен в документе «Регламент обеспечения безопасности персональных данных».

11.2. Управление доступом третьих сторон к персональным данным.

11.2.1. КПК «Регион-Финанс» в ходе своей деятельности осуществляет предоставление доступа (в т. ч. осуществляет передачу) к ПДн третьим лицам в целях исполнения договорных обязательств перед своими контрагентами и субъектами ПДн, а также с целью обеспечения своей деятельности или исполнения требований нормативных документов РФ. При этом субъект ПДн может беспрепятственно получить доступ к перечню третьих сторон, которым предоставляется доступ к его ПДн, если это не противоречит требованиям законодательства РФ.

11.2.2. КПК «Регион-Финанс» передаются ПДн только в объеме, необходимом для достижения заявленных целей обработки.

11.2.3. Существенным условием договоров с третьими сторонами, в рамках исполнения которых предоставляется доступ к ПДн, является обязанность соблюдения сторонами мер обеспечения безопасности ПДн при их обработке. Кроме того, в договорах в обязательном порядке определяется порядок передачи ПДн.

11.3. Поручение обработки персональных данных.

11.3.1. КПК «Регион-Финанс» может поручать обработку ПДн другим лицам (третьим сторонам), а также выступать в роли лица, осуществляющего обработку ПДн по поручению других операторов ПДн.

11.3.2. КПК «Регион-Финанс» поручает обработку ПДн третьим сторонам только с согласия субъекта ПДн или при наличии иного законного основания (договор с субъектом ПДн) при обязательном условии соблюдения стороной, осуществляющей обработку ПДн по поручению КПК «Регион-Финанс», соблюдения правил обработки и обеспечения безопасности ПДн, установленных КПК «Регион-Финанс».

11.3.3. При обработке ПДн по поручению третьих сторон КПК «Регион-Финанс» соблюдаются установленные соответствующими поручениями (договорами) требования к обеспечению безопасности ПДн.

11.3.4. В поручении на обработку ПДн должны быть в обязательном порядке определены:

- перечень действий (операций) с персональными данными, которые будут совершаться лицом (перечень действий не должен противоречить целям и действиям, заявленным перед субъектом - в договоре, согласии и т. д.);
- цели обработки (цели не должны противоречить целям, заявленным перед субъектом - в договоре, в согласии и т. д.);
- обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
- требования к защите ПДн (требования по защите, предъявляемые к лицу, осуществляющему обработку, не должны быть выше требований, выполняемых самим оператором – в идеальном случае требования должны быть идентичны).

12. ВЗАИМОДЕЙСТВИЕ С СУБЪЕКТАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОРГАНАМИ ВЛАСТИ

12.1. Взаимодействие с субъектами

12.1.1. Порядок взаимодействия с субъектами ПДн или их законными представителями описан в документе «Регламент взаимодействия с субъектами персональных данных».

12.2. Взаимодействие с органами власти

12.2.1. Взаимодействие с органами власти осуществляется в соответствии с законодательством РФ.

12.2.2. Оценка законности и мотивированности запросов органов власти на предоставление информации о процессах обработки ПДн (в т. ч. на предоставление ПДн) проводится Ответственным за организацию обработки ПДн.

12.2.3. При взаимодействии с органами власти обязательным является подача уведомления в уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку ПДн.

12.2.4. Подача Уведомления осуществляется в порядке, предусмотренном п. 13.1. Форма и детальный состав Уведомления определяется в соответствии с нормативными документами Уполномоченного органа по защите прав субъектов ПДн. Ответственным за подачу Уведомления является Ответственный за организацию обработки ПДн.

12.2.5. Контроль необходимости внесения изменений в Уведомление осуществляется в рамках мероприятий по модернизации и внутреннему контролю СЗПДн, описанных в документе «Регламент обеспечения безопасности персональных данных».

12.2.6. Уполномоченным органом по защите прав субъектов ПДн (основным регулятором в сфере обработки ПДн) является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор). Роскомнадзор, в частности, уполномочен:

- осуществлять проверку сведений, содержащихся в Уведомлении, и привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

- обращаться к операторам с требованиями по уточнению, блокированию или уничтожению недостоверных или полученных незаконным путем ПДн;

- принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований п. 13.1.;

- направлять в ФСБ России и ФСТЭК России сведения о мерах по обеспечению безопасности ПДн, указанных в Уведомлении;

- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

- привлекать к административной ответственности лиц, виновных в нарушении требований п. 13.1.

12.2.7. ФСБ России и ФСТЭК России могут быть наделены решением Правительства РФ полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности ПДн, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных. В т. ч. это касается отдельных решений Правительства РФ о проведении контрольных мероприятий.

13. НОРМАТИВНЫЕ ССЫЛКИ

13.1. В настоящем документе использованы ссылки на следующие нормативные правовые акты:

13.1.1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

13.1.2. 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».

13.1.3. 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.

13.1.4. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».