УТВЕРЖДЕНО

Общим собранием СКПК «Денежный поток»

Протокол №2 от 30.09.2019г.

Положение
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК»

Якутск
2019

СОДЕРЖАНИЕ

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее "Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», далее – Положение, регламентирует - правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений СКПК «ДЕНЕЖНЫЙ ПОТОК» (далее по тексту – Организация) законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. Термины, используемые в настоящем Плане, применяются в тех значениях, которые определены в законодательстве, нормативных правовых актах, указанных в настоящем Плане и иных нормативных правовых актах, а также:

ПДн – персональные данные;

ИСПДн – информационные системы, в которых обрабатываются персональные данные;

МНИ – материальный носитель информации;

СА – системный администратор, подразделение Организации, объединяющее системных администраторов, а также подразделения Организации, включая сотрудников, отвечающие в Организации за информационную безопасность.

ЗД – заместитель директора Организации, ответственное лицо за обработку персональных данных.

СТАТЬЯ 1. ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

– Гражданский кодекс Российской Федерации (далее – ГК РФ);

– Трудовой кодекс Российской Федерации (далее – ТК РФ);

– Налоговый кодекс Российской Федерации (далее – НК РФ);

– Федеральный закон от 27.07.2006 № 152 – ФЗ "О персональных данных" (далее – Закон 152–ФЗ, Федеральный закон "О персональных данных");

– Федеральный закон от 27.07.2006 №149 – ФЗ "Об информации, информационных технологиях и о защите информации";

– Федеральный закон от 07.08.2001 года № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма" (далее– Закон 115-ФЗ);

– Постановление Правительства РФ от 15.09.2008 года № 687 "Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

– Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

СТАТЬЯ 2. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Для выявления и предотвращения нарушений, предусмотренных законодательством Российской Федерации в сфере персональных данных, в Организации используются следующие процедуры:

2.1.1. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

2.1.2. Оценка вреда, который может быть причинен субъектам персональных данных;

2.1.3. Ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с законодательством Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящим Положением и (или) обучение по соответствующим дополнительным профессиональным программам;

2.1.4. Осуществление обработки персональных данных в соответствии с принципами и условиями обработки персональных данных, установленными законодательством Российской Федерации в сфере персональных данных;

2.1.5. Недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

2.1.6. Обеспечение при обработке персональных данных точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных.

2.1.7. Ограничение обработки персональных данных достижением конкретных, заранее определенных и законных целей.

2.1.8. Ограничение сроков хранения в форме, позволяющей определить субъекта персональных данных, требованиями 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.

2.1.9. Уничтожение либо обезличивание по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

СТАТЬЯ 3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

3.1. В Организации, персональные данные обрабатывают в следующих целях:

3.1.1. Для осуществления возложенных на Организацию законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: "О микрофинансовой деятельности и микрофинансовых организациях", "О кредитных историях", "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма", "О рынке ценных бумаг", "О несостоятельности (Банкротстве)", "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования", "О персональных данных", нормативными актами Организации России, а также Уставом и правовыми актами Организации;

3.1.2. Для организации учета сотрудников Организации для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия сотруднику в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами 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 Организации.

3.1.3. Персональные данные обработанные на официальном сайте Кооператива (www.skpk.denpotok.ru) через сервис Яндекс.Метрика предоставляемый компанией ООО «Яндекс» (ИНН: 7736207543, ОГРН: 1027700229193) используется с целью анализа пользовательской активности на сайте Общества. Передаваемые персональные данные являются обезличенными и не позволяют идентифицировать конкретного посетителя сайта Общества.

3.1.4. Во всех перечисленных случаях Организации необходимо получить согласие субъектов персональных данных на их обработку, за исключением случаев, перечисленных в пункте 2 статьи 6 Федерального закона "О персональных данных".

СТАТЬЯ 4. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сроки обработки указанных выше персональных данных определяются в соответствие со сроком действия договора с субъектом ПДн, сроком исковой давности, а также иными требованиями законодательства и нормативными документами Организации России, а также локальных правовых актов Организации, регламентирующих порядок хранения документов.

Кооператив через сервис Яндекс.Метрика использует информацию, содержащуюся в файлах cookie только в указанных выше целях, после чего собранные данные будут храниться на устройстве пользователя в течение периода, который может зависеть от соответствующего типа файлов cookie, но не превышая срока, необходимого для достижения их цели, после чего они будут автоматически удалены из системы пользователя.

СТАТЬЯ 5. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

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

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

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

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

СТАТЬЯ 6. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом. Обработка персональных данных допускается в следующих случаях:

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

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее – исполнение судебного акта);

4) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

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

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

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в 15 Федерального закона «О персональных данных», при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных);

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

6.2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно Федеральным законом "О персональных данных".

6.3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключае-

мого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом "О персональных данных". В поручении оператора должны быть определены перечень действий (операций) с персональными данными, 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 в соответствии с Федеральным законом "О персональных данных".

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

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

СТАТЬЯ 7. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

СТАТЬЯ 8. ОБЩЕДОСТУПНЫЕ ИСТОЧНИКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

8.2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

СТАТЬЯ 9. СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБРАБОТКУ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. 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, информированным и сознательным. Согласие на обработку персональных данных 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 на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

9.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Федеральный закон "О персональных данных".

9.3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в Федеральном законе "О персональных данных".

9.4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

2) 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 доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

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

4) цель обработки персональных данных;

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

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

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

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

9) подпись субъекта персональных данных.

9.5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

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

9.7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

9.8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в Федеральном законе "О персональных данных".

СТАТЬЯ 10. СПЕЦИАЛЬНЫЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния

здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

10.2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные сделаны общедоступными субъектом персональных данных;

3) в иных случаях, установленных законом.

3. Обработка персональных данных специальных категорий, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

СТАТЬЯ 11. БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

11.1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

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

СТАТЬЯ 11-1 ОБЕЗЛИЧЕННЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

11-1.1 Обработка обезличенных персональных данных производится на официальном сайте www.denpotok.ru с помощью сервиса Яндекс.Метрика с целью анализа пользовательской активности на сайте.

11-1.2 Обработка обезличенных персональных данных осуществляется с согласия субъекта персональных данных.

Согласие субъекта персональных данных при передачи данных через сервис Яндекс.Метрика:

При посещении официального сайта Общества автоматически всплывает сообщение о предупреждении о том, что сайт использует сервис веб-аналитики Яндекс.Метрика, которая использует технологию «cookie» - текстовые файлы, размещаемые на компьютере пользователя с целью анализа их пользовательской активности.

Субъект ПДн в праве отказаться от использования «cookie», выбрав соответствующие настройки в браузере, а также установить блокировку по ссылке https://yandex.ru/support/metrica/general/opt-out.html.

Общество для анализа пользовательской активности на сайте использует следующие типы файлов:

статистические / аналитические файлы cookie: эти файлы cookie позволяют распознавать пользователей, подсчитывать их количество;

технические файлы cookie: эти файлы cookie собирают информацию о том, как пользователи взаимодействуют с Сайтами и/или Сервисами, что позволяет выявлять ошибки и тестировать новые функции для повышения производительности Сайтов и Сервисов; идентифицируют аппаратное и программное обеспечение, включая тип браузера.

СТАТЬЯ 12. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с Федеральным законом "О персональных данных" и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

12.2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

12.3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

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

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

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

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

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

СТАТЬЯ 13. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННЫХ ИЛИ МУНИЦИПАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

13.2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

13.3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

13.4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

ГЛАВА 2. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

СТАТЬЯ 14. ПРАВО СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ДОСТУП К ЕГО ПЕРСОНАЛЬНЫМ ДАННЫМ

14.1. Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

14.2. Сведения, указанные в части 7 настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

14.3. Сведения, указанные в части 7 настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

14.4. В случае, если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

14.5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса.

14.6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

14.7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников/агентов оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

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

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

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

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

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

10) иные сведения, предусмотренные Федеральным законом "О персональных данных" или другими федеральными законами.

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

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

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

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

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

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

СТАТЬЯ 15. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ ИХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ПРОДВИЖЕНИЯ ТОВАРОВ, РАБОТ, УСЛУГ НА РЫНКЕ, А ТАКЖЕ В ЦЕЛЯХ ПОЛИТИЧЕСКОЙ АГИТАЦИИ

15.1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

15.2. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в части 1 настоящей статьи.

СТАТЬЯ 16. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПРИНЯТИИ РЕШЕНИЙ НА ОСНОВАНИИ ИСКЛЮЧИТЕЛЬНО АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

16.1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных частью 2 настоящей статьи.

16.2. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

16.3. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

16.4. Оператор обязан рассмотреть возражение, указанное в части 3 настоящей статьи, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

СТАТЬЯ 17. ПРАВО НА ОБЖАЛОВАНИЕ ДЕЙСТВИЙ ИЛИ БЕЗДЕЙСТВИЯ ОПЕРАТОРА

17.1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

ГЛАВА 3. ОБЯЗАННОСТИ ОПЕРАТОРА

СТАТЬЯ 18. ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ СБОРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

18.1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную Федеральным законом "О персональных данных".

18.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

18.3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные Федеральным законом "О персональных данных» права субъекта персональных данных;

5) источник получения персональных данных.

4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

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

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

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 настоящей статьи, нарушает права и законные интересы третьих лиц.

18.3. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом "О персональных данных» или другими федеральными законами. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с Федеральным законом "О персональных данных";

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону "О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных", соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных";

6) ознакомление работников/агентов оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников/агентов.

18.4. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

18.5. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

СТАТЬЯ 19. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

19.1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

19.2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

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

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

19.3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

19.4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обес-

печения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

19.5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Организация России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

19.6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

19.7. Проекты нормативных правовых актов, указанных в части 5 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

19.8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

19.9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

19.10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от не-

правомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

19.11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

СТАТЬЯ 20. ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ ОБРАЩЕНИИ К НЕМУ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ПРИ ПОЛУЧЕНИИ ЗАПРОСА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ЕГО ПРЕДСТАВИТЕЛЯ, А ТАКЖЕ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

20.1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона «О персональных данных», субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

20.1.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона "О персональных данных" или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

20.1.3. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

20.1.4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

СТАТЬЯ 21. ОБЯЗАННОСТИ ОПЕРАТОРА ПО УСТРАНЕНИЮ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА, ДОПУЩЕННЫХ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПО УТОЧНЕНИЮ, БЛОКИРОВАНИЮ И УНИЧТОЖЕНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом "О персональных данных" или другими федеральными законами.

5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не

превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом "О персональных данных" или другими федеральными законами.

6. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 – 5 настоящей статьи, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

СТАТЬЯ 22. УВЕДОМЛЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

22.1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

22.2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) сделанных субъектом персональных данных общедоступными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

22.3. Уведомление, предусмотренное частью 1 настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

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

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

22.4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

22.5. На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.

22.6. В случае предоставления неполных или недостоверных сведений, указанных в части 3 настоящей статьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

22.7. В случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

СТАТЬЯ 23 ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

23.1. Оператор распорядительным документов назначает лицо, ответственное за организацию информационной безопасности в Организации, который отвечает за обработку персональных данных.

23.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от Руководителя Организации (лица, исполняющего его обязанности), и подотчетно ему.

23.3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 Федерального закона "О персональных данных".

23.4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников/агентов оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

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

ГЛАВА 4. КОНТРОЛЬ И НАДЗОР ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА

СТАТЬЯ 24. УПОЛНОМОЧЕННЫЙ ОРГАН ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

24.1. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

24.2. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

24.3. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований Федерального закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;

6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

7) 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;

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

9) привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона;

10) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в пункте 7 части 3 статьи 22 Федерального закона "О персональных данных".

24.4. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

24.5. Уполномоченный орган по защите прав субъектов персональных данных обязан:

1) организовывать в соответствии с требованиями Федерального закона и других федеральных законов защиту прав субъектов персональных данных;

2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений;

3) вести реестр операторов;

4) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;

5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;

6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;

7) выполнять иные предусмотренные законодательством Российской Федерации обязанности.

24.6. Уполномоченный орган по защите прав субъектов персональных данных осуществляет сотрудничество с органами, уполномоченными по защите прав субъектов персональных данных в иностранных государствах, в частности международный обмен информацией о защите прав субъектов персональных данных, утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

24.7. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

24.8. Уполномоченный орган по защите прав субъектов персональных данных ежегодно направляет отчет о своей деятельности Президенту Российской Федерации, в Правительство Российской Федерации и Федеральное Собрание Российской Федерации. Указанный отчет подлежит опубликованию в средствах массовой информации.

24.9. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета.

24.10. При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

СТАТЬЯ 25. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА

25.1. Лица, виновные в нарушении требований Федерального закона "О персональных данных", несут предусмотренную законодательством Российской Федерации ответственность.

25.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

ГЛАВА 5. ОСНОВНЫЕ ЗАДАЧИ ОРГАНИЗАЦИИ, ЭКСПЛУАТИРУЮЩЕЙ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

СТАТЬЯ 26. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРЫ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ НЕПРАВОМЕРНОГО ИЛИ СЛУЧАЙНОГО ДОСТУПА К НИМ, УНИЧТОЖЕНИЯ, ИЗМЕНЕНИЯ, БЛОКИРОВАНИЯ, КОПИРОВАНИЯ, РАСПРОСТРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ ОТ ИНЫХ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ

Во всех внедряемых информационных системах с момента их ввода в эксплуатацию должна обеспечиваться защита персональных данных. В отношении действующих информационных систем, обрабатывающих персональные данные, Организация при эксплуатации системы обязан решить следующие задачи:

1. Провести классификацию ИСПДн с оформлением соответствующего акта.

2. Реализовать комплекс мер по защите персональных данных в соответствии с перечисленными правовыми актами и методическими документами.

3. Провести оценку соответствия ИСПДн требованиям безопасности в форме сертификации (аттестации) или декларирования соответствия.

Решение поставленных задач достигается совместной работой подразделений Организации.

Статья 27. Разграничение прав доступа к персональным данным работников/агентов

Права доступа к персональным данным в Организации имеют:

– Руководитель Организации и его заместители (ко всем получаемым в Организации ПДн Субъектов);

– работники/агенты отдела кадров (доступ к ПДн работников/агентов Организации, информация о фактическом месте проживания и контактные телефоны работников/агентов);

– работники/агенты бухгалтерии (информация о ПДн клиентов Организации, полученная в ходе осуществления операций, а также информация, полученная при расчетах с работниками Организации);

– работники/агенты Службы внутреннего контроля (доступ ко всем получаемым в Организации ПДн Субъектов при осуществлении внутреннего контроля);

– работники/агенты Административно-хозяйственного отдела (ПДн о Субъектах, полученная при исполнении должностных обязанностей);

– руководители и работники/агенты иных структурных подразделений Организации, филиалов (ВСП) Организации по направлению деятельности (доступ к персональным данным только с целью исполнения должностных обязанностей).

СТАТЬЯ 28. СОСТАВЛЕНИЕ ПЕРЕЧНЯ СИСТЕМ ОРГАНИЗАЦИИ, В КОТОРЫХ ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

28.1. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных".

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

28.3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

28.4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных".

28.5. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

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

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

28.7. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

28.8. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

28.9. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

28.10. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

28.11. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

28.12. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

28.13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

28.14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 28.13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

28.15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 28.14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников/агентов) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

28.16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных 28.15, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

28.17. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Статья 29. Принятие решения о вводе в действие Отраслевой модели угроз.

29.1. В качестве модели угроз безопасности персональных данных при их обработке в ИСПДн Организация использует Отраслевую модель угроз, содержащую актуальные угрозы безопасности персональных данных при обработке в ИСПДн Организации и согласованную с Регуляторами.

29.2 В случае необходимости, по требованию заинтересованных работников/агентов Организации, участвующих в обработке персональных данных, по распоряжению руководства Организации производится разработка собственной частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных Организации.

29.3. В соответствии с пунктом 16 Порядка проведения классификации информационных систем персональных данных, утвержденного приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" для специальных информационных систем персональных данных должна быть разработана модель угроз безопасности персональных данных.

29.4. В случае необходимости, в Организации может быть составлена частная модель угроз безопасности персональных данных при их обработке в ИСПДн Организации (далее – частная модель угроз), учитывающая особенности обработки персональных данных в Организации с учетом складывающейся практики.

В качестве методики выбора актуальных для Организации угроз и последующего составления частной модели угроз используются рекомендации в области стандартизации Организации России РС БР ИББС-2.2-2009 "Обеспечение информационной безопасности организаций БС Российской Федерации. Методика оценки рисков нарушения информационной безопасности.

Статья 30. Оценка возможности обезличивания персональных данных

Персональные данные, обрабатываемые в ИСПДн, можно обезличить с целью понижения уровня требований по обеспечению безопасности. Согласно Федеральному закону "О персональных данных" обезличивание – это действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Полностью обезличить все персональные данные невозможно – в информационных системах всегда будут присутствовать технические средства (например, автоматизированные рабочие места или принтеры), на которых будет происходить процесс, обратный обезличиванию, – для целей сверки данных, печати на принтере, отправки по электронной почте и т.п.

На основе анализа национальных и международных стандартов может быть составлен следующий список алгоритмов обезличивания персональных данных.

На момент утверждения настоящего Положения в Организации объективно отсутствует возможность обезличивания персональных данных, однако создается методика, позволяющая это осуществить.

Персональные Данные полученные сайте Общества с помощью сервиса Яндекс.Метрика полностью обезличены.

Статья 31. Оценка существующих защитных мер на предмет соответствия требованиям Стандартов Организации России

ГЛАВА 6. ДЕКЛАРИРОВАНИЕ СООТВЕТСТВИЯ

Декларирование соответствия – это подтверждение соответствия характеристик информационной системы персональных данных предъявляемым к ней требованиям, установленным законодательством Российской Федерации, руководящими и нормативно-методическими документами ФСТЭК России и ФСБ России.

Декларирование соответствия может осуществляться на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии.

В случае проведения декларирования на основе собственных доказательств Организация самостоятельно формирует комплект документов, таких как техническая документация, другие документы и результаты собственных исследований, послужившие мотивированным основанием для подтверждения

соответствия информационной системы персональных данных всем необходимым требованиям, предъявляемым к классу К3.

Независимо от используемой формы подтверждения соответствия Организация может также предоставить протоколы испытаний, проведенных в исследовательской лаборатории.

Декларации о соответствии, полученные на основе собственных доказательств и с участием третьей стороны имеют одинаковую юридическую силу. Также они имеют действие, аналогичное действию сертификата (аттестата) соответствия, и также действительны на территории всей страны и стран, признающих разрешительные документы системы ГОСТ Р в течение всего срока действия.

Декларация о соответствии оформляется на русском языке и должна содержать:

– наименование и местонахождение заявителя;
– наименование и местонахождение изготовителя;
– информацию об объекте подтверждения соответствия, позволяющую идентифицировать этот объект;
– наименование документа, на соответствие требованиям которого подтверждается продукция;
– указание на схему декларирования соответствия;
– заявление заявителя о безопасности продукции при ее использовании в соответствии с целевым назначением и принятии заявителем мер по обеспечению соответствия продукции требованиям технических регламентов;
– сведения о проведенных исследованиях (испытаниях) и измерениях, сертификате системы качества, а также документах, послуживших основанием для подтверждения соответствия продукции требованиям технических регламентов;
– срок действия декларации о соответствии.

Срок действия декларации о соответствии определяется техническим регламентом.

Форма декларации о соответствии утверждается федеральным органом исполнительной власти по техническому регулированию.

ГЛАВА 7. ПРОЦЕДУРЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИЕЙ, В ТОМ ЧИСЛЕ ИСПДн

СТАТЬЯ 1. КРИТЕРИИ ОТНЕСЕНИЯ АС К ИСПДН

1.1. Критерии отнесения АС к ИСПДн в Организации:

– наличие ПДн в базах данных АС;
– Организация является оператором ПДн в АС.

1.2. Классификация информационных систем

1.2.1. Классификацию АС, используемых Организацией в технологических процессах, осуществляет СА по классификации ПДп. Результаты классификации оформляются в виде Перечня ИСПДн Организации в которых обрабатываются персональные данные (Приложение № 4).

ИСПДн Организации классифицируются на основе категории обрабатываемых в ИСПДн данных. Отдельной графой выделяются следующие категории:

1). ИСПДн обработки специальных категорий ПДн.

2) ИСПДн обработки биометрических ПДн

3) ИСПДн обработки ПДн, которые не могут быть отнесены к специальным категориям ПДн, биометрическим ПДн, общедоступным или обезличенным.

4) ИСПДн обработки общедоступных и/или обезличенных ПДн.

СТАТЬЯ 2. ПРОЦЕДУРЫ УЧЕТА РЕСУРСОВ ПДН

2.1.С целью учета ресурсов ПДн, в том числе учета ИСПДн в Организации в соответствии с внутренними документами, в том числе с настоящим Положением, выполняются, регистрируются и контролируются следующие процедуры учета ресурсов ПДн, в том числе учета ИСПДн:

2.2. Учет ресурсов ПДн без использования средств автоматизации, и АС устанавливается внутренними документами Организации с учетом сроков обработки персональных данных и требований законодательства.

2.3. Учет ресурсов ПДн с использованием средств автоматизации, и АС регистрируется СА в Акте классификации информационных систем (Приложение № 5), далее – Акт классификации ИС, который ежегодно контролируется и при необходимости пересматривается.

Учет средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов осуществляется путем заполнения Журнала (Приложения №№ 6, 11).

2.4. Для каждого ресурса ПДн должно быть обеспечено:

– установление цели обработки ПДн;
– установление и соблюдение сроков хранения ПДн и условий прекращения их обработки;
– определение перечня и категорий, обрабатываемых ПДн (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн);
– выполнение процедур учета количества субъектов ПДн, в том числе субъектов ПДн, не являющихся работниками Организации;
– выполнение ограничения обработки ПДн достижением цели обработки ПДн;
– соответствие содержания и объема обрабатываемых ПДн установленным целям обработки;
– точность, достаточность и актуальность ПДн, в том числе по отношению к целям обработки ПДн;
– выполнение установленных процедур получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн в случае, если получение такого согласия необходимо в соответствии с требованиями закона;
– выполнение установленных процедур получения согласия субъектов ПДн на передачу обработки их ПДн третьим лицам в случае, если получение такого согласия необходимо в соответствии с требованиями закона;
– прекращение обработки ПДн и уничтожение либо обезличивание ПДн (Приложение № 1) по достижении целей обработки, по требованию субъекта ПДн в случаях, предусмотренных законом, в том числе при отзыве субъектом ПДн согласия на обработку его ПДн.

2.5. При работе с материальными носителями ПДн Организация обеспечивает:

– обособление ПДн от иной информации, в частности, путем фиксации их на отдельных съемных носителях ПДн, в специальных разделах или на полях форм документов (при обработке ПДн на бумажных носителях);
– учет съемных носителей ПДн (при их использовании);
– порядок хранения съемных, в том числе машинных, носителей ПДн и доступа к ним, а также уничтожения (стирания) информации с машинных носителей ПДн;
– хранение ПДн, цели обработки которых заведомо несовместимы, на отдельных съемных носителях (при их использовании);
– регистрацию и учет мест хранения материальных носителей ПДн с фиксацией категории обрабатываемых ПДн (иные ПДн), включая раздельное хранение ресурсов ПДн, обработка которых осуществляется с различными целями;

СТАТЬЯ 3. ПРОЦЕДУРЫ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПДН

3.1. В Организации должны выполняться, регистрироваться и контролироваться процедуры учета лиц, имеющих доступ к ПДн.

Безопасность ИСПДн в Организации достигается путем исключения несанкционированного, в том числе случайного доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

Обработка ПДн работниками Организации должна осуществляться только с целью выполнения их должностных обязанностей.

3.2. Организация для защиты ПДн субъектов принимает комплекс мер, направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий. К таким мерам, в том числе, относятся:

– назначение лица, ответственного за организацию обработки ПДн;
– определение угроз безопасности ПДн при их обработке в ИСПДн;
– применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн;
– применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
– оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
– учет машинных носителей ПДн;
– обнаружение фактов несанкционированного доступа к ПДн и принятием мер;
– восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
– установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
– контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн;
– иные меры по решению Руководителя Организации.

3.3. Список лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей установлен Приложением № 3.

3.4. Сотрудники, имеющие доступ к ПДн, обязаны их использовать только в целях, для которых эти ПДн получены, и обязаны соблюдать режим конфиденциальности.

3.5. Организация предоставляет субъекту ПДн или его представителю доступ к его ПДн при обращении или при получении письменного запроса от него или его представителя.

СТАТЬЯ 4. ПРОЦЕДУРЫ ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ПДН С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИХ ТОЧНОСТИ, ДОСТОВЕРНОСТИ И АКТУАЛЬНОСТИ, В ТОМ ЧИСЛЕ ПО ОТНОШЕНИЮ К ЦЕЛЯМ ОБРАБОТКИ ПДН

4.1. Все обрабатываемые Организацией ПДн должны быть точны, актуальны и достоверны.

4.2. Формы документов Организации, определяющие порядок взаимодействия с работниками Организации и третьими лицами должны содержать положения о необходимости предоставления субъектом ПДн сведений об изменениях, внесенных в ПДн, представленных им Организации.

4.3. Работники/агенты Организации обязаны при выполнении возложенных на них функций

осуществлять контроль точности, актуальности и достоверности персональных данных, обрабатываемых Организацией, сверяясь с общедоступными источниками информации.

СТАТЬЯ 5. ПРОЦЕДУРЫ УНИЧТОЖЕНИЯ, ОБЕЗЛИЧИВАНИЯ ЛИБО БЛОКИРОВАНИЯ ПДН В СЛУЧАЕ НЕОБХОДИМОСТИ ВЫПОЛНЕНИЯ ТАКИХ ПРОЦЕДУР

5.1. В Организации должны выполняться, регистрироваться и контролироваться процедуры прекращения обработки ПДн, их уничтожение либо обезличивание в сроки, установленные законом, в следующем порядке:

5.1.1. Организация осуществляет блокирование ПДн субъектов или обеспечивает блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) в случаях:

– выявления неправомерной обработки ПДн, неточных ПДн при обращении субъекта ПДн или его представителя, либо по запросу субъекта ПДн или его представителя или Роскомнадзора на период проверки данного обстоятельства;

– отсутствия возможности уничтожения ПДн либо обезличивания ПДн в течение срока, установленного Федеральным законом № 152-ФЗ. Блокирование осуществляется на срок не более 6 (Шести) месяцев с последующим обеспечением уничтожения ПДн.

– подтверждения факта неточности ПДн Организация на основании сведений, предоставленных субъектом ПДн или его представителем или Роскомнадзором, или иных необходимых документов, уточняет или обеспечивает (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) уточнение соответствующих ПДн в течение 7 (Семи) рабочих дней со дня предоставления таких сведений в Организацию и снимает блокирование ПДн.

5.1.2. Процедуры прекращения обработки ПДн, их уничтожение либо обезличивание осуществляются в соответствии настоящей Статьей и с Приложениями №№ 1, 20 в следующих случаях:

– по достижении цели обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн, иным соглашением между Организацией и субъектом ПДн);

– отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн, иным соглашением между Фондом и субъектом ПДн);

– если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

– выявления неправомерной обработки ПДн, осуществляемой Организацией или обработчиком, действующим по его поручению, если обеспечить правомерность обработки ПДн невозможно;

– выявления неправомерной обработки ПДн без согласия субъекта ПДн.

В случае отсутствия возможности уничтожения ПДн либо обезличивания ПДн в течение срока, установленного законом, Организация обеспечивает их блокирование с последующим обеспечением уничтожения ПДн. Уничтожение ПДн производится не позднее шести месяцев со дня их блокирования.

5.2. Блокирование, уничтожение и обезличивание ПДн, МНИ ПДн осуществляется в соответствии с Приложением № 20 комиссией, состоящей из руководителя подразделения, осуществляющего обработку ПДн, подлежащих блокированию, уничтожению и/или обезличиванию, и СА.

5.3. Результаты уничтожения и обезличивания носителей ПДн оформляются актом (Приложение № 10, 13, 21).

СТАТЬЯ 6. ПРОЦЕДУРЫ ОБРАБОТКИ ОБРАЩЕНИЙ И ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНЫХ ЛИЦ

6.1. Обработка обращений субъектов ПДн (их законных представителей) для случаев, предусмотренных Федеральным законом «О персональных данных», в частности порядок подготовки информации о наличии ПДн, относящихся к конкретному субъекту ПДн, информации, необходимой для предоставления возможности ознакомления субъектом ПДн (их законных представителей) с его ПДн, а также процедуры обработки обращений об уточнении ПДн, их блокировании или уничтожении, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для установленной цели обработки, осуществляется в соответствии Регламентом реагирования на обращения субъектов персональных данных; запросы Уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных (Приложение № 17).

6.2. Типовые формы ответа на запросы приведены в Приложении № 19.

6.3. Сведения об обращениях субъектов персональных данных и иных лиц, получающих доступ к персональным данным, заносятся работниками Организации, ответственных за обработку запросов и обращений в Журнал учета обращений субъектов персональных данных (Приложение № 9).

СТАТЬЯ 7. ПРОЦЕДУРЫ ПОЛУЧЕНИЯ СОГЛАСИЯ СУБЪЕКТА ПДН НА ОБРАБОТКУ ЕГО ПДН И НА ПЕРЕДАЧУ ОБРАБОТКИ ЕГО ПДН ТРЕТЬИМ ЛИЦАМ

7.1. Перед началом обработки ПДн работник, уполномоченный распорядительным документов, трудовым договором и/или должностной инструкцией Организации обязан получить согласие субъекта ПДН.

7.2. Согласие субъекта ПДн на обработку персональных данных оформляется путем заполнения формы (Приложение № 8), если иная форма не предусмотрена законодательством, либо иными внутренними документами Организации для отдельных ситуаций.

7.3. Согласие на обработку персональных данных, заполненное и подписанное субъектом ПДн хранится в соответствии с порядком, установленным внутренними документами Организации в течение срока обработки ПДн Организацией.

СТАТЬЯ 8. ПРОЦЕДУРЫ ПЕРЕДАЧИ ПДН МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ РЕСУРСА ПДН, ПРЕДУСМАТРИВАЮЩИЕ ПЕРЕДАЧУ ПДН ТОЛЬКО МЕЖДУ РАБОТНИКАМИ ОРГАНИЗАЦИИ, ИМЕЮЩИМИ ДОСТУП К ПДН

8.1. В случае необходимости разграничения доступа к ПДн, обрабатываемых пользователями ресурса ПДн в Организации, работник Организации, уполномоченный на обработку ПДн устанавливает наличие прав подразделения, получающего доступ к ресурсу, содержащему ПДн, на обработку ПДн.

8.2. Объем передаваемых в пределах Организации персональных данных должен быть ограничен теми данными, которые необходимы для выполнения целей передачи и функций получающего их работника.

8.3. Передача ресурсов, содержащих персональные данные, фиксируется документально в Журнале учета передачи ресурсов, содержащих ПДн, работниками Организации (Приложение № 18).

СТАТЬЯ 9. ПРОЦЕДУРЫ УЧЕТА ПОМЕЩЕНИЙ, В КОТОРЫХ ОБРАБАТЫВАЮТСЯ ПДН А ТАКЖЕ ДОПУСКА В НИХ

9.1. Все помещения Организации, в которых осуществляется обработка ПДн, подлежат учету,

который отражается в Журнале учета помещений, в которых обрабатываются персональные данные, а также допуска в них (Приложение № 15).

9.2. Доступ работников/агентов Организации в помещения, в которых обрабатываются персональные данные, строго ограничен наличием у работника прав на обработку персональных данных, которые хранятся и обрабатываются в помещении.

9.3. Материальные носители персональных данных хранятся в помещениях, физическая защита которых и собственно технических средств АС осуществляется с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в них посторонних лиц, хищение документов и информационных носителей персональных данных.

9.4. Помещения Организации, в которых осуществляется обработка ПДн, должны быть оборудованы техническими средствами охраны, которые включают в свой состав:

– средства охранной сигнализации;
– средства пожарной сигнализации;
– инженерно-технические средства защиты (укрепленные двери, замки, шкафы, запирающиеся на ключ).

9.5. За сохранность и недоступность для посторонних лиц информации о персональных данных в указанных помещениях ответственность несут работники/агенты Организации , осуществляющие обработку персональных данных в указанных помещениях на основании распоряжения руководства Организации .

9.6. Ежедневный контроль выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных осуществляют начальники соответствующих подразделений.

9.7. Доступ в помещение, в котором осуществляется обработка персональных данных, посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находиться в помещении только в присутствии сотрудников Организации, имеющих право находиться в помещении, в связи с выполнением своих должностных обязанностей.

9.8. Доступ в помещение в неурочное время или в выходные и праздничные дни осуществляется на основании письменного разрешения Руководителя Организации.

9.9. Доступ в помещение, в котором обрабатываются ПДн, лиц, не являющихся работниками Организации, оформляется разовыми пропусками. Сведения о выдаче разовых пропусков вносятся в Журнал учета разовых пропусков (Приложение № 7).

СТАТЬЯ 10. ПРОЦЕДУРЫ ПЕРЕДАЧИ ПДН ТРЕТЬИМ ЛИЦАМ

10.1. Передача ПДн третьим лицам, включение ПДн в общедоступные источники, их распространение или поручение обработки другому лицу осуществляется только при наличии письменного согласия субъекта ПДн на эти действия, за исключением случаев, предусмотренных законодательством Российской Федерации.

10.2. Организация не осуществляет передачу ПДн в коммерческих целях.

10.3. Договор, заключаемый с лицом, осуществляющим обработку ПДн по поручению Организации должен содержать:

– обязательство лица соблюдать принципы и правила обработки ПДн, предусмотренные законодательством;

– перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки;

– ответственность лица за действия, связанные с обработкой ПДн.

10.4. Третьи лица, получающие от Организации ПДн, должны гарантировать использованик ПДн только в тех целях, для которых они сообщены, обеспечивать защиту полученных ПДн. Организация вправе требовать от третьих лиц подтверждения выполнения требований к защите ПДн.

СТАТЬЯ 11. ПРОЦЕДУРЫ РАБОТЫ С МАТЕРИАЛЬНЫМИ НОСИТЕЛЯМИ ПДН

11.1. Организация осуществляет хранение ПДн на материальных носителях. Срок хранения ПДн определен внутренними документами Организации, если иное не установлено законодательством, либо договором, стороной которого является Организация. В иных случаях хранение ПДн не может осуществляться дольше, чем этого требуют цели обработки ПДн.

11.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации для каждой категории персональных данных должен использоваться отдельный материальный носитель.

11.3. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

– при необходимости использования или распространения определенных персональных данных отдельно от находящихся из том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копня персональных данных;

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

11.4. При работе с МНИ ПДн должно быть обеспечено:

– обособление ПДн от иной информации, в частности путем фиксации их на отдельных МНИ ПДн, в специальных разделах или на полях форм документов (при обработке ПДн на бумажных носителях);

– хранение ПДн, цели обработки которых заведомо несовместимы, на отдельных МНИ;

– регистрация и учет мест хранения МНИ ПДн с фиксацией категории обрабатываемых персональных данных (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн), включая раздельное хранение ресурсов ПДн, обработка которых осуществляется с различными целями;

– установление и выполнение порядка гарантированного уничтожения (стирания) информации с МНИ ПДн.

11.5. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.

СТАТЬЯ 12. ПРОЦЕДУРЫ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ УВЕДОМЛЕНИЯ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПДН ОБ ОБРАБОТКЕ ПДН В СРОКИ, УСТАНОВЛЕННЫЕ ЗАКОНОМ

12.1. Организация уведомляет уполномоченный орган по защите прав субъектов ПДн об осуществлении обработки ПДн согласно Статье 22 Федерального закона № 152-ФЗ.

12.2. В случае изменения сведений, указанных в части 3 Статьи 22 Федерального закона № 152-ФЗ, а также в случае прекращения обработки ПДн Организация обязана уведомить об этом уполномоченный орган по защите прав субъектов ПДн в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн.

12.3. Ответственным за направление уведомлений в соответствии с настоящей Статьей является заместитель Директора.

СТАТЬЯ 13. НЕОБХОДИМОСТЬ ПРИМЕНЕНИЯ ТИПОВЫХ ФОРМ ДОКУМЕНТОВ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАБОТКИ ПДН И ПРОЦЕДУРЫ РАБОТЫ С НИМИ

13.1. Под типовой формой документа понимается шаблон, бланк документа или другая унифицированная форма документа, используемая Организацией с целью сбора ПДн.

13.2. С целью соблюдения требований к обработке персональных данных Организация обязана осуществлять процедуры, предусмотренные настоящим Положением и иными внутренними документами с применением бланков (форм), установленных для этих целей.

13.3. При разработке и использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональные данные, должны соблюдаться следующие условия:

13.3.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование Организации, 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 Организацией способов обработки персональных данных.

13.3.2. При необходимости получения письменного согласия субъекта на обработку персональных данных типовая форма должна предусматривать поле, в которой субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации.

13.3.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные, содержатся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая нрав и законных интересов иных субъектов персональных данных.

13.4. Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

13.5. Работники/агенты Организации при осуществлении процедур, предусмотренных настоящим Положением, обязаны осуществлять заполнение и применение форм, приведенных в приложениях к настоящему Положению. Ответственными за использование той или иной формы является руководитель подразделения, в функции которого входит ее использование.

СТАТЬЯ 14. ПРОЦЕДУРЫ ОЗНАКОМЛЕНИЯ РАБОТНИКОВ/АГЕНТОВ/АГЕНТОВ ОРГАНИЗАЦИИ С ТРЕБОВАНИЯМИ К ОБРАБОТКЕ ПДН

14.1. В ходе проведения мероприятий по обучению или повышению осведомленности работников/агентов не реже одного раза в два года в Организации проводится ознакомление работников/агентов с положениями законодательства и внутренними документами Организации, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

14.2. Работники/агенты Организации, непосредственно осуществляющие обработку ПДн, обязаны быть ознакомлены с положениями законодательства Российской Федерации и внутренними документами Организации, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

14.3. Ознакомление работников/агентов производит СА в следующих случаях:

– при внесении изменений в положения законодательства Российской Федерации и/или внутренние документы Организации, содержащих требования по обработке и обеспечению безопасности ПДн;
– не реже одного раза в два года.

14.4. Регистрация ознакомления работников/агентов в соответствии с настоящей статьей осуществляется в Журнале регистрации сведений об ознакомлении работников/агентов с информацией по обработке персональных данных в соответствии с Приложением № 12.

14.5. На СА возлагается контроль за соблюдения процедур ознакомления работников/агентов в соответствии с настоящей статьей.

СТАТЬЯ 15. ПРОЦЕДУРЫ ПУБЛИКАЦИИ ПДН В ОБЩЕДОСТУПНЫХ ИСТОЧНИКАХ ПДН

15.1. Общедоступные источники ПДн создаются и публикуются Организацией только для цели выполнения требований законодательства Российской Федерации.

15.2. Материалы для публикации в общедоступных источниках, содержащие ПДн должны согласовываться с Руководителем Организации.

15.3. При формировании и публикации информации, содержащей ПДн в общедоступных источниках ПДн следует учитывать все требования законодательства к форме и содержанию публикации.

15.4. Регистрация публикации ПДн в общедоступных источниках ПДн отражается в Журнале публикации ПДн в общедоступных источниках ПДн (Приложение № 14).

15.5. Контроль за соблюдением процедур, установленных настоящей статьей, осуществляет СА.

СТАТЬЯ 16. ПРОЦЕДУРЫ ПОРУЧЕНИЯ ОБРАБОТКИ ПДН ТРЕТЬЕМУ ЛИЦУ

16.1. Поручение обработки ПДн третьему лицу (далее – обработчик) должно осуществляться в соответствии с требованиями законодательства на основании договора.

16.2. В указанном договоре должны быть определены перечень действий (операций) с ПДн, которые будут совершаться обработчиком, и цели обработки, должна быть установлена обязанность обработчика обеспечивать безопасность ПДн (в том числе соблюдать конфиденциальность ПДн) при их обработке, не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом, а также должны быть указаны требования по обеспечению безопасности ПДн.

16.3. При поручении обработки ПДн обработчику Организация должна получить согласие субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.

СТАТЬЯ 17. ПРОЦЕДУРЫ ВЫПОЛНЯЕМЫЕ В СЛУЧАЯХ НЕОБХОДИМОСТИ ОСУЩЕСТВЛЕНИЯ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ПДН

17.1. В случаях необходимости осуществления трансграничной передачи ПДн, работник Организации, ответственный за обработку ПДн, обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

17.2. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, осуществляется в случаях:

1) наличия в Организации согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

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

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

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

17.3. Сведения об осуществлении в Организации трансграничной передачи ПДн заносятся в Журнал регистрации трансграничной передачи ПДн лицом, ответственным за обработку ПДн.

17.4. Контроль за соблюдением процедур, установленных настоящей статьей несет СА.

СТАТЬЯ 18. ОТВЕТСТВЕННОСТЬ

18.1. Лицом, ответственным за организацию обработки ПДн в Организации, является ЗД.

18.2. С целью исполнения настоящего Положения ЗД наделяется следующими полномочиями:

– контролировать исполнение работниками Организации исполнения требований, установленных к обработке ПДн законодательством, настоящим Положением, иными нормативными документами и локальными правовыми актами;

– требовать от работников/агентов Организации исполнения законодательства, настоящего Положения и иных нормативных документов, и локальных правовых актов, регламентирующих порядок обработки ПДн;

– осуществлять ознакомление работников/агентов Организации с законодательством, настоящим Положением и иными нормативными документами, и локальными правовыми актами, регламентирующими порядок обработки ПДн.

18.3. ЗД в целях исполнения настоящего Положения имеет право:

– получать от работников/агентов Организации необходимые документы, справки, отчеты, свидетельствующие об исполнении настоящего Положения;

– посещать помещения, в которых обрабатываются персональные данные,

– осуществлять проверку действий и документов в целях, установленных настоящим Положением.

18.4. ЗД обязан:

соблюдать требования законодательства, настоящего Положения и иных нормативных документов и локальных правовых актов, регламентирующих порядок обработки ПДн.

18.5. Ответственность за контроль исполнения и поддержание Политики в актуальном состоянии, а также за внесение в нее изменений возлагается на ЗД.

18.6. Ответственность за организацию хранения материальных носителей ПДн возлагается на ЗД.

18.7. Все работники/агенты Организации несут персональную ответственность за соблюдение требований Положения.

СТАТЬЯ 19. ПРОЧИЕ ПОЛОЖЕНИЯ, ПОРЯДОК ПЕРЕСМОТРА И ВНЕСЕНИЯ ИЗМЕНЕНИЙ

19.1. В случае отмены и/или изменения норм законодательства Положение действует в части, не противоречащей действующему законодательству Российской Федерации, при этом Организация в разумные сроки вносит в Положение соответствующие изменения.

19.2. Организация должна опубликовать настоящее Положение на сайте Организации в сети Интернет, а также разместить на информационном стенде в офисе Организации с целью обеспечения к нему неограниченного доступа.

ПРИЛОЖЕНИЯ:

Приложение № 1. Алгоритмы обезличивания персональных данных (ПДн);

Приложение № 2. Перечень персональных данных, обрабатываемых в Организации;

Приложение № 3. Список лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей;

Приложение № 4. Перечень ИСПДн Организации в которых обрабатываются персональные данные;

Приложение № 5. Акт классификации информационных систем персональных данных;

Приложение № 6. Журнал учета носителей персональных данных;

Приложение № 7. Журнал учета разовых пропусков;

Приложение № 8. Согласие на обработку персональных данных;

Приложение № 9. Журнал учета обращений граждан (субъектов ПДн) о выполнении ими законных прав в области защиты ПДн;

Приложение № 10. Акт уничтожения носителей персональных данных;

Приложение № 11. Журнал учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов;

Приложение № 12. Журнал регистрации сведений об ознакомлении работников/агентов с информацией по обработке персональных данных;

Приложение № 13. Акт о комиссионном уничтожении криптографических ключей;

Приложение № 14. Журнал публикации ПДн в общедоступных источниках ПДн;

Приложение № 15. Журнал учета помещений, в которых обрабатываются персональные данные, а также допуска в них;

Приложение № 16. Порядок и условия обработки специальных категорий и биометрических персональных данных, порядок и условия трансграничной передачи персональных данных, порядок обработки персональных данных, осуществляемой без использования средств автоматизации);

Приложение № 17. Регламент реагирования на обращения субъектов персональных данных; запросы уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных ;

Приложение № 18. Журнал учета передачи ресурсов, содержащих ПДн, работниками Организации;

Приложение № 19. Типовая форма ответа на запросы;

Приложение № 20. Инструкция по уничтожению ПДн;

Приложение № 21. Акт об обезличивании в Организации персональных данных.

Приложение 1
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Алгоритмы обезличивания персональных данных (ПДн)

Алгоритм обезличивания	Описание	Примечание
Абстрагирование ПДн	Сделать ПДн менее точными путем группирования общих или непрерывных характеристик	Например, вместо указания конкретного возраста использовать кодификаторы (18-25 лет – 2, 26-33 года – 3 и т.д.)
Скрытие ПДн	Удалить все или часть записи ПДн, не требуемой для деятельности кредитной организации	
Внесение шума в ПДн	Добавить небольшое количество посторонней информации в ПДн	
Замена ПДн	Переставить поля одной записи ПДн с теми же самыми полями другой аналогичной записи	
Замена данных средним значением	Заменить выбранные данные средним значением для группы ПДн	
Разделение ПДн на части	Использование таблиц перекрестных ссылок	Например, вместо одной таблицы использовать две – одна с ФИО и идентификатором субъекта ПДн, вторая – с тем же идентификатором субъекта ПДн и остальной частью ПДн
Использование специальных алгоритмов	Маскирование ПДн или подмена определенных символов другими	
Использование алгоритмов криптографического преобразования	Хэширование или шифрование	

Приложение 2
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному Протоколом Общего Собрания №2 от «30» сентября 2019 года.

Перечень персональных данных, обрабатываемых в Организации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Перечень персональных данных, подлежащих защите в СКПК «ДЕНЕЖНЫЙ ПОТОК» (далее – Перечень), разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ "О персональных данных".

2. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Сведениями, составляющими персональные данные, в Организации является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:

2.1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

2.3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность.

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

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

2.6. Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, 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).

2.7. 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 окончании образовательного учреждения и другие сведения).

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

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

2.10. Содержание и реквизиты трудового договора с работником Организации или гражданско-правового договора с гражданином.

2.11. Сведения о заработной плате (номера счетов для расчета с работниками, данные зарплатных договоров с клиентами, в том числе номера их картсчетов, данные по окладу, надбавкам, налогам и другие сведения).

2.12. 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).

2.13. 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).

2.14. Сведения об имуществе (имущественном положении):

– автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств);

– недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость, полные адреса размещения объектов недвижимости и другие сведения);

– банковские вклады (данные договоров с клиентами, в том числе номера их счетов, картсчетов, вид, срок размещения, сумма, условия вклада и другие сведения);

– кредиты (займы), 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).

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

2.16. Сведения об идентификационном номере налогоплательщика.

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

2.18. Сведения, указанные в оригиналах и копиях приказов по личному составу Организации и материалах к ним.

2.19. 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) работников/агентов Организации.

2.20. Материалы по аттестации и оценке работников/агентов Организации.

2.21. Материалы по внутренним служебным расследованиям в отношении работников/агентов Организации.

2.22. Материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами.

2.23. Сведения о временной нетрудоспособности работников/агентов Организации.

2.24. Табельный номер работника Организации.

2.25. 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).

5. КЛАССИФИКАЦИЯ ОБРАБАТЫВАЕМЫХ В ОРГАНИЗАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СООТВЕТСТВИИ СО СТЕПЕНЬЮ ТЯЖЕСТИ ПОСЛЕДСТВИЙ ПОТЕРИ СВОЙСТВ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Выделяются следующие категории персональных данных:

– персональные данные, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным;

– персональные данные, отнесенные в соответствии с Федеральным законом "О персональных данных" к общедоступным или обезличенным персональным данным.

Приложение 3
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Список лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей

Перечень (список) работников/агентов, осуществляющих обработку персональных данных в ИСПДн (либо имеющих доступ к персональным данным) регламентируется:

– распорядительными документами Организации, содержащими предоставление работникам прав доступа в ИСПДн (приказами, распоряжениями руководства Организации);

– перечнем, распечатанным на бумажном носителе в виде поименной базы пользователей в случае необходимости (в частности, перед проведением проверок);

– допуском работников/агентов к персональным данным, обрабатываемым в ИСПДн, на ролевой основе в соответствии с занимаемой должностью в случаях, установленных внутренними документами Организации.

В этом случае к обработке персональных данных в ИСПДн считаются допущенными те работники/агенты Организации, характер служебных обязанностей которых в соответствии с должностными инструкциями, положениями о подразделениях, в которых числятся работники/агенты, иными внутренними документами Организации, а также исходя из сложившейся практики и обстановки, предполагает обработку персональных данных в информационных системах Организации.

Настоящий перечень подлежит корректировке, расширению и пересмотру в зависимости от меняющихся целей и задач Организации.

Возможно существование перечня (списка) в электронном виде при условии предоставления работникам прав доступа в ИСПДн только на основании распорядительного документа в документально зафиксированном в Организации порядке.

Приложение 4
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Перечень ИСПДн Организации в которых обрабатываются персональные данные

Все информационные системы Организации оцениваются руководителями структурных подразделений Организации на возможность отнесения к системам обработки персональных данных.

Классификация ИСПДн осуществляется с учетом категорий и объема накапливаемых, обрабатываемых и распределяемых с их использованием ПДн с целью установления методов и средств защиты, необходимых для обеспечения безопасности ПДн.

Состав и функциональное содержание методов и средств защиты зависит от вида и степени ущерба, возникающего вследствие реализации угроз безопасности ПДн. При этом ущерб возникает за счет неправомерного или случайного уничтожения, изменения, блокирования, копирования, распространения ПДн или от иных неправомерных действий с ними. В зависимости от объекта, причинение ущерба которому, в конечном счете, вызывается неправомерными действиями с ПДн, рассматриваются два вида ущерба: непосредственный и опосредованный.

Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту ПДн. Он возникает за счет незаконного использования (в том числе распространения) ПДн или за счет несанкционированной модификации этих данных и может проявляться в виде:

– нанесения вреда здоровью субъекта ПДн;

– незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;

– потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПДн;

– нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь путем осуществления контактов с ним по различным поводам без его на то согласия (например – рассылка персонифицированных рекламных предложений и т.п.).

Опосредованный ущерб связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности экономических, политических, военных, медицинских, правоохранительных, социальных, кредитно-финансовых и иных государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с ПДн.

Критерии отнесения автоматизированной системы к информационным системам персональных данных (ИСПДн) в Организации приведены в Таблице 1.

Таблица 1

№ класса	Наименование системы	Цель создания ИСПДн	Разработчик ИСПДн	Эксплуатирующее ИСПДн подразделение	Исходные данные*
1	2	3	4	5	6
1.	**Обработка платежей по обязательствам с клиентами**	**расчеты с клиентами**	**Организация**	**подразделения Организации, отвечающие за обработку платежей клиентов**	Перечень персональных данных, которые обрабатываются в ИСПДн: 1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения. 2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство. 3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность. 4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания. Категория обрабатываемых персональных данных – общедоступные Объем обрабатываемых персональных данных – количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн: не лимитирован, Виды и цели обработки персональных данных – сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных; Характеристики безопасности: – Конфиденциаль-

* Содержание столбца определяется решением комиссии по приведению Организации в соответствие требованиям Федерального закона "О персональных данных"

					ность, – целостность, – доступность. Структура ИСПДн: автономные. Наличие подключения ИСПДн к сетям связи общего пользования и сетям международного информационного обмена: не имеет подключений. Режим обработки персональных данных: многопользовательские. Режим разграничения прав доступа пользователей к ИСПДн: системы с разграничением прав доступа (доступ имеют только лица, должностные обязанности которых непосредственно связаны с обработкой персональных данных). Местонахождение технических средств ИСПДн – все технические средства которых находятся в пределах Российской Федерации.
2.	**Сбербанк Бизнес-онлайн, АЭБ-Бизнес**	**Перевод денежных средств по расчетам Организации**	**ПАО Сбербанк, АКБ «АЭБ» АО**	**Бухгалтерия Организации**	Перечень персональных данных, которые обрабатываются в ИСПДн: 1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения. 2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство. 3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность. 4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания. Категория обрабатываемых персональных

					данных – общедоступные Объем обрабатываемых персональных данных – количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн: _____. Виды и цели обработки персональных данных – сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных; Характеристики безопасности: – Конфиденциальность, – целостность, – доступность. Структура ИСПДн: автономные. Наличие подключения ИСПДн к сетям связи общего пользования и сетям международного информационного обмена: не имеет подключений. Режим обработки персональных данных: многопользовательские. Режим разграничения прав доступа пользователей к ИСПДн: системы с разграничением прав доступа (доступ имеют только лица, должностные обязанности которых непосредственно связаны с обработкой персональных данных). Местонахождение технических средств ИСПДн – все технические средства которых находятся в пределах Российской Федерации.
3.	**Ведение досье клиентов**	**_____**	**_____**	**подразделения Организации, отвечающие за ра-**	Перечень персональных данных, которые обрабатываются в ИСПДн:

				боту с клиентами клиентов	1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения. 2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство. 3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность. 4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания. Категория обрабатываемых персональных данных – общедоступные Объем обрабатываемых персональных данных – количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн: не лимитирован Виды и цели обработки персональных данных – сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных; Характеристики безопасности: – Конфиденциальность, – целостность, – доступность. Структура ИСПДн: автономные. Наличие подключения ИСПДн к сетям связи общего пользования и сетям международного информационного обмена: не имеет подключений.

					Режим обработки персональных данных: многопользовательские. Режим разграничения прав доступа пользователей к ИСПДн: системы с разграничением прав доступа (доступ имеют только лица, должностные обязанности которых непосредственно связаны с обработкой персональных данных). Местонахождение технических средств ИСПДн – все технические средства которых находятся в пределах Российской Федерации.
4.	**Ведение личных дел работников/агентов**	**_____**	**_____**	**кадровая служба Организации**	Перечень персональных данных, которые обрабатываются в ИСПДн: 1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения. 2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство. 3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность. 4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания. Категория обрабатываемых персональных данных – общедоступные Объем обрабатываемых персональных данных – количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн: не лимитирован Виды и цели обработки

					персональных данных – сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных; Характеристики безопасности: – Конфиденциальность, – целостность, – доступность. Структура ИСПДн: автономные. Наличие подключения ИСПДн к сетям связи общего пользования и сетям международного информационного обмена: не имеет подключений. Режим обработки персональных данных: многопользовательские. Режим разграничения прав доступа пользователей к ИСПДн: системы с разграничением прав доступа (доступ имеют только лица, должностные обязанности которых непосредственно связаны с обработкой персональных данных). Местонахождение технических средств ИСПДн – все технические средства которых находятся в пределах Российской Федерации.
5.	**Сбор информации на сайте Когоператива**	**Для анализа пользовательской активности на сайте Общества**	**ООО «Яндекс»**	**Системный администратор**	статистические / аналитические файлы cookie: эти файлы cookie позволяют распознавать пользователей, подсчитывать их количество; технические файлы cookie: эти файлы cookie собирают информацию о том, как пользователи взаимодействуют с Сайтами и/или Сервисами, что позволяет выявлять

					ошибки и тестировать новые функции для повышения производительности Сайтов и Сервисов; идентифицируют аппаратное и программное обеспечение, включая тип браузера.

Приложение 5
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

АКТ
классификации информационных систем персональных данных в Организации

№ п/п	Наименование ИСПДн	Цель создания ИСПДн (цель обработки ПДн)	Разработчик ИСПДн	Эксплуатирующее ИСПДн подразделение	Исходные данные ИСПДн	Класс ИСПДн
1	2	3	4	5	6	7
1	АРМ	**расчеты с клиентами**	_____	СА	Перечень персональных данных, которые обрабатываются в ИСПДн: 1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения. 2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство. 3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность. 4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания. Категория обрабатываемых персональных данных – общедоступные Объем обрабатываемых персональных данных – количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн: 40 Виды обработки персональных данных – сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных; Характеристики безопасности: – Конфиденциальность, – целостность, – доступность. Структура ИСПДн: автономные. Наличие подключения ИСПДн к сетям связи общего пользования и сетям международного информационного обмена: не имеет подключений. Режим обработки персональных данных:	В соответствии с определенными критериями классификации – класс 3 и класс 4

1	2	3	4	5	6	7
					многопользовательские. Режим разграничения прав доступа пользователей к ИСПДн: системы с разграничением прав доступа (доступ имеют только лица, должностные обязанности которых непосредственно связаны с обработкой персональных данных). Местонахождение технических средств ИСПДн – все технические средства которых находятся в пределах Российской Федерации.	
2	**Сбербанк Бизнес-онлайн, АЭБ-Бизнес**	**Перевод денежных средств по расчетам Организации**	_____	**бухгалтерия Организации**	Перечень персональных данных, которые обрабатываются в ИСПДн: 1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения. 2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство. 3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность. 4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания. Категория обрабатываемых персональных данных – общедоступные Объем обрабатываемых персональных данных – количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн: не лимитирован Виды обработки персональных данных – сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных; Характеристики безопасности: – Конфиденциальность, – целостность, – доступность. Структура ИСПДн: автономные. Наличие подключения ИСПДн к сетям связи общего пользования и сетям международного информационного обмена: не имеет подключений. Режим обработки персональных данных: многопользовательские. Режим разграничения прав доступа пользователей к ИСПДн: системы с разграничением прав доступа (доступ имеют только лица, должностные обязанности которых непосредственно связаны с обработкой персональных данных).	В соответствии с определенными критериями классификации – класс 3 и класс

1	2	3	4	5	6	7
					Местонахождение технических средств ИСПДн – все технические средства которых находятся в пределах Российской Федерации.	
3	**АРМ**	**сбор и хранение информации о клиентах**	_____	**подразделение Организации, ответственное за работу с клиентами**	Перечень персональных данных, которые обрабатываются в ИСПДн: 1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения. 2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство. 3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность. 4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания. Категория обрабатываемых персональных данных – общедоступные Объем обрабатываемых персональных данных – количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн: 300 Виды обработки персональных данных – сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных; Характеристики безопасности: – Конфиденциальность, – целостность, – доступность. Структура ИСПДн: автономные. Наличие подключения ИСПДн к сетям связи общего пользования и сетям международного информационного обмена: не имеет подключений. Режим обработки персональных данных: многопользовательские. Режим разграничения прав доступа пользователей к ИСПДн: системы с разграничением прав доступа (доступ имеют только лица, должностные обязанности которых непосредственно связаны с обработкой персональных данных). Местонахождение технических средств ИСПДн – все технические средства которых находятся в пределах Российской Федерации.	В соответствии с определенными критериями классификации – класс 3 и класс
3	**АРМ**	**сбор и хранение информации**	_____	**кадровая служба Организации**	Перечень персональных данных, которые обрабатываются в ИСПДн: 1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.	В соответствии с определенными кри-

1	2	3	4	5	6	7
		работниках			2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство. 3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность. 4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания. Категория обрабатываемых персональных данных – общедоступные Объем обрабатываемых персональных данных – количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн: 300 Виды обработки персональных данных – сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных; Характеристики безопасности: – Конфиденциальность, – целостность, – доступность. Структура ИСПДн: автономные. Наличие подключения ИСПДн к сетям связи общего пользования и сетям международного информационного обмена: не имеет подключений. Режим обработки персональных данных: многопользовательские. Режим разграничения прав доступа пользователей к ИСПДн: системы с разграничением прав доступа (доступ имеют только лица, должностные обязанности которых непосредственно связаны с обработкой персональных данных). Местонахождение технических средств ИСПДн – все технические средства которых находятся в пределах Российской Федерации.	терриями классификации – класс 3 и класс 4
4	**Яндекс.Метрика**	**Для анализа пользовательской активности на сайте Кооператива**	**ООО «Яндекс»**	**Системный администратор**	статистические / аналитические файлы cookie: эти файлы cookie позволяют распознавать пользователей, подсчитывать их количество; технические файлы cookie: эти файлы cookie собирают информацию о том, как пользователи взаимодействуют с Сайтами и/или Сервисами, что позволяет выявлять ошибки и тестировать новые функции для повышения производительности Сайтов и Сервисов; идентифицируют аппаратное и программное обеспе-	В соответствии с определенными критериями классификации – класс 4

1	2	3	4	5	6	7
					чение, включая тип браузера.	

Приложение 6
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Приложение 6.
Журнал учета носителей персональных данных

Журнал начат "____" _____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен "____" _____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п/п	Регистрационный номер	Дата учета	Тип / емкость носителя	Серийный номер	Отметка о постановке на учет (ФИО, подпись, дата)	Отметка о снятии с учета (ФИО, подпись, дата)	Местоположение носителя	Сведения об уничтожении носителя / стирании информации
1	2	3	4	5	6	7	8	9

Приложение 7

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Журнал учета разовых пропусков

Журнал начат "____" _____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен "____" _____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

Номер пропуска	**Номер заявки на выдачу пропусков**	**ФИО посетителя**	**Наименование принимающего структурного подразделения**	**ФИО должностного лица, подписавшего пропуск**	**Время начала действия пропуска**	**Вид документа, с которым пропуск действителен**	**Место посещения 8**	**9 Фактическое время выхода**	**Отметка о возврате пропуска**	**Подпись дежурного бюро пропусков**
1.	2	3	4	5	6	7	8	9	10	11
2.										
3.										
4.										

Приложение 8
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Согласие на обработку персональных данных (КЛИЕНТ)

Я, _____

(фамилия, имя, отчество — субъекта персональных данных)

в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", даю согласие Сельскохозяйственному кредитному потребительскому кооперативу «Денежный поток» (677009, г. Якутск, ул. Дзержинского д.11, офис 4) и его уполномоченным представителям на обработку и использование моих персональных данных, содержащихся в настоящем заявлении, с целью получения займа, исполнения Договора Займа, Договора поручительства, где поручителем выступает заявитель, информировании об услугах СКПК «Денежный поток». При этом под моими персональными данными понимаются относящиеся ко мне сведения и информация (фамилия, имя, отчество, дата и место рождения, адреса места жительства, семейное, социальное положение, сведения о занятости, имуществе, доходах, кредитная история, фотография, контактные данные, реквизиты документов), любые данные предоставленные мною в т. ч. указанные в настоящем заявлении.

Основной документ: Паспорт гражданина Российской Федерации серия _____ № _____
кем выдан: _____
код подразделения: _____
Дата рождения: _____
Место рождения: _____
Адрес регистрации: _____
Адрес проживания: _____
Телефоны: Тел.: Сотовый: _____, Рабочий: _____, Рабочий: _____, Родственник: _____
Место работы: _____
Доход в месяц: _____
Должность: _____
ИНН: _____
СНИЛС: _____

1. Заявитель осознает и принимает ответственность за дачу заведомо ложных сведений в соответствии с Федеральным законом «О кредитных историях».
2. Заявитель настоящим дает свое согласие СКПК «Денежный поток» на обработку, хранение, передачу персональных данных Заявителя и иной информации, связанной с возможным предоставлением займа Заявителю, заключением договора поручительства, где поручителем выступает заявитель, исполнением Заявителем обязанностей по возврату займа, в Бюро кредитных историй, в том числе сведений, указанных в ст. 4 Федерального закона «О кредитных историях», и иных сведений, указанных Заявителем в настоящем заявлении. Заявитель также настоящим дает свое согласие и уполномочивает СКПК «Денежный поток» получать кредитные отчеты в отношении себя (Заявителя) в Бюро кредитных историй в порядке, установленном Федеральным законом «О кредитных историях». Данное разрешение действует в течение трех лет со дня подписания настоящего документа, а в случае заключения договора займа или договора поручительства между СКПК «Денежный поток» и Заявителем, в течение всего срока действия указанного договора. В случае неисполнения Заявителем своих обязательств по указанному договору, Заявитель дает согласие на распространение персональных данных, указанных в настоящем заявлении третьим лицам.
3. Обработка вышеуказанных персональных данных будет осуществляться путем смешанной обработки персональных данных (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение использования, распространение), в том числе передача), обезличивание, блокирование, уничтожение персональных данных.
4. Согласно п.2. ст. 9 ФЗ N 152-ФЗ "О персональных данных" Заявитель вправе отозвать согласие на обработку персональных данных, на основании личного заявления.
5. При обработке персональных данных СКПК «Денежный поток» руководствуется ФЗ «О персональных данных» и ФЗ «О кредитных историях».
6. Заявитель согласен с информированием о состоянии расчетов по займу и услугах СКПК «Денежный поток» с использованием любых каналов связи в т.ч. электронных сообщений (sms, электронная почта).

Согласие выдано: Подпись_____ дата _____

Выдача повторных согласий (Подписанием подтверждаю выдачу согласия на указанные сроки. В случае если дата окончания согласия не заполняется, заявитель подтверждает выдачу согласия на три года с указанной даты выдачи согласия)

Дата выдачи	Дата окончания согласия	Подпись	Фамилия И.О.

Согласие
на обработку персональных данных (для работников/агентов)

Я, _____ (далее Субъект),
(ФИО субъекта персональных данных)
зарегистрирован _____,
(адрес субъекта персональных данных)
_____,
(данные паспорта (или иного документа, удостоверяющего личность)
не возражаю против обработки СКПК «ДЕНЕЖНЫЙ ПОТОК» (далее Оператор), расположенным по адресу: _____, моих персональных данных на следующих условиях:

1. Субъект даёт согласие на обработку своих персональных данных, как с использованием средств автоматизации, так и без использования таких средств, т.е. совершение, в том числе следующих действий: сбор, систематизацию, накопление, хранение, уточнение, использование, блокирование, уничтожение, а также право на передачу такой информации третьим лицам и получение информации и документов от третьих лиц для осуществления проверки достоверности и полноты информации о Субъекте и в случаях, установленных законодательством.

2. Перечень персональных данных Субъекта, передаваемых Оператору на обработку:

1) ФИО;
2) паспортные данные;
3) дата рождения;
4) место рождения;
5) адрес регистрации;

3. Согласие даётся Субъектом с целью проверки корректности предоставленных субъектом сведений, принятия решения о предоставлении Субъекту услуг, для заключения с Оператором любых договоров и их дальнейшего исполнения, принятия решений или совершения иных действий, порождающих юридические последствия в отношении Субъекта и иных лиц.

4. Обработка персональных данных (за исключением хранения) прекращается по достижению цели обработки или прекращения обязательств по заключённым договорам и соглашениям или исходя из документов Оператора, регламентирующих вопросы обработки персональных данных.

5. Настоящее согласие действует до даты его отзыва мною путем направления в СКПК «ДЕНЕЖНЫЙ ПОТОК» письменного сообщения об указанном отзыве в произвольной форме, если иное не установлено законодательством Российской Федерации. В этом случае оператор прекращает обработку персональных данных Субъекта, а персональные данные подлежат уничтожению, если отсутствуют иные правовые основания для обработки, установленные законодательством Российской Федерации или документами Оператора, регламентирующих вопросы обработки персональных данных.

6. Данное согласие действует в течение всего срока обработки персональных данных до момента, указанного в п.4 или п.5 данного согласия.

" " 20 г. _____ _____
(подпись) (ФИО)

Приложение 9
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Журнал учета обращений граждан (субъектов ПДн) о выполнении ими законных прав в области защиты ПДн

Журнал начат "____" _____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен "____" _____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи / отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8
1.							
2.							
3.							

Приложение 10
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Разрешаю уничтожить
<руководитель структурного подразделения или должностное лицо, ответственное за обеспечение безопасности ПДн>
_____
подпись ФИО
"___" _____200__ г.

Акт уничтожения носителей персональных данных

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего подлежит уничтожению _____
(цифрами и прописью)

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

После утверждения акта перечисленные носители ПДн сверены с записями в акте и уничтожены путем _____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии: _____ / /

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

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

Приложение 11

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Журнал учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Журнал начат "____"
_____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен "____"
_____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п.п.	Наименование СКЗИ	Регистрационные номера СКЗИ,	Отметка о получении		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств ИСПДН			Примечание
			От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ 8	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	12	13	14	15
1											
2											
3											
4											
5											
6											
7											

Приложение 12
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Журнал

регистрации сведений об ознакомлении работников/агентов с информацией по обработке персональных данных

Журнал начат "____"
_____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен "____"
_____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п.п.	Должность работника, осуществляющего обработку ПДн	ФИО работника, осуществляющего обработку ПДн	Дата ознакомления с информацией по обработке ПДн	Должность и ФИО работника, проводившего ознакомление	Подпись работника, проводившего ознакомление
1	2	3	4		

Приложение 13
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Утверждаю
<руководитель структурного подразделения или должностное лицо, ответственное за обеспечение безопасности ПДн>
_____
подпись ФИО
"___" _____200__ г.

Акт
о комиссионном уничтожении криптографических ключей

Комиссия в составе:

	ФИО	**Должность**
Председатель		
Члены комиссии		

провела уничтожение криптографических ключей:

№ п/п	**Дата**	**Тип носителя ключа**	**Регистрационный номер носителя ключа**	**Наименование СКЗИ**	**Примечание**

Всего носителей **криптографических ключей**:
_____
(цифрами и прописью)

На указанных носителях криптографические ключи уничтожены путем _____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители криптографических ключей уничтожены путем _____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель комиссии: _____ / /

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

Приложение 14
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Журнал
публикации ПДн в общедоступных источниках ПДн

№ п/п	Сведения о публикуемом документе	Источник публикации	Должность и ФИО работника, ответственного за публикацию	Цель публикации	Подпись лица, указанного в графе 4 Журнала
1	2	3	4	5	6

Приложение 15
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Журнал
учета помещений, в которых обрабатываются персональные данные, а также допуска в них

№ п/п	Описание помещения, в котором обрабатываются ПДн	Должность и ФИО работника, имеющих допуск в помещение, указанное в графе 2 Журнала	Должность и ФИО работника, осуществляющего контроль за допуском в помещение, указанное в графе 2 Журнала Цель передачи Подписи лиц, указанных в графах 3 и 4 Журнала
1	2	3	4

Приложение 16
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Порядок и условия обработки специальных категорий и биометрических персональных данных, порядок обработки персональных данных, осуществляемой без использования средств автоматизации)

1. Получение специальных категорий персональных данных и биометрических персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации, нормативными и распорядительными документами Организации России, локальными правовыми актами Организации и настоящим Положением и не допускается, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных".

2. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка персональных данных для исполнения трудовых договоров или без использования средств автоматизации и в иных случаях, предусмотренных законодательством Российской Федерации.

3. Обработка и использование персональных данных, указанных в пункте 2 настоящего Порядка (далее – "ПД») осуществляется в целях, указанных в соглашениях с субъектами ПД, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации. Не допускается принятие на основании исключительно автоматизированной обработки ПД решений, порождающих юридические последствия в отношении субъекта ПД или иным образом затрагивающих его права и законные интересы.

4. В случае увольнения субъекта ПД и иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Организации обязана незамедлительно прекратить обработку ПД и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки ПД, если иное не предусмотрено настоящим Положением.

5. ПД могут храниться в бумажном и (или) электронном виде, а также на магнитных и иных носителях, централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных. Право на обработку ПД предоставляется по занимаемой должности работникам, в должностные обязанности которых входит такая обработка, либо обработка документации, содержащей соответствующие сведения, а также персонально иным лицам в соответствии с приказами по Организации или письменными указаниями руководства Организации.

6. Порядок и условия обработки и использования ПД, включая сроки хранения содержащих персональные данные оригиналов документов или копий документов на записываемых оптических носителях, предназначенных для архивного хранения, устанавливаются приказами, регламентами и инструкциями по Организации при наличии деятельности по обработке таких ПД. Правила обработки и использования электронных копий ПД на иных носителях, включая сроки их хранения, могут конкретизироваться в инструкциях по использованию соответствующих информационных систем.

7. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Организации.

Приложение 17
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Регламент реагирования на обращения субъектов персональных данных; запросы уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных

1. Настоящий Регламент разработан в соответствии с от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (далее – Закон № 152-ФЗ).

Регламент устанавливает единый порядок рассмотрения и разрешения в Организации обращений граждан Российской Федерации, иностранных граждан, лиц без гражданства, обращений и запросов должностных и иных лиц о предоставлении доступа к персональным данным.

2. Порядок доступа граждан Российской Федерации, иностранных граждан и лиц без гражданства, проживающих на территории Российской Федерации, регламентируется соответствующими нормами законодательства.

3. Порядок приема, учета, регистрации обращений (запросов), их оформления, размножения, систематизации и хранения, а также контроля за их исполнением устанавливается локальными правовыми актами Организации по делопроизводству.

4. При рассмотрении обращения не допускается разглашение содержащихся в нем сведений.

5. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации, а также иную информацию согласно требованиям Закона № 152-ФЗ.

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

1) подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

2) способы обработки персональных данных, применяемые оператором;

3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

4) перечень обрабатываемых персональных данных и источник их получения;

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

6) сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

7. Субъект персональных данных имеет право на получение сведений о Организации о месте его нахождения, о наличии у Организации персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными, за исключением случаев, предусмотренных частью 5 настоящей Законом № 152-ФЗ. Субъект персональных данных вправе требовать от Организации уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случаях, установленных Законом № 152-ФЗ.

9. Организация обязана в порядке, предусмотренном Законом № 152-ФЗ, сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

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

11. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных Организация обязана дать в письменной форме мотивированный ответ, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо с даты получения запроса субъекта персональных данных или его законного представителя.

12. Организация обязана безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Организация обязана уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

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

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

15. Запросы и обращения субъектов персональных данных разрешаются при участии подразделений Организации, осуществляющих их обработку.

16. Организация обязана сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение семи рабочих дней с даты получения такого запроса.

17. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

1) запрашивать у Организации информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от Организации уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;

6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

7) 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;

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

9) привлекать к административной ответственности лиц, виновных в нарушении Федерального закона "О персональных данных".

18. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

Приложение 18

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Журнал учета передачи ресурсов, содержащих ПДн, работниками Организации

№ п/п	Вид ресурса, содержащего ПДн	Должность и ФИО работника, передающего ресурс, содержащий ПДн	Должность и ФИО работника, получающего ресурс, содержащий ПДн	Цель передачи	Подписи лиц, указанных в графах 3 и 4 Журнала
1	2	3	4	5	6

Приложение 19

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Типовая форма ответа на запросы

Ответ Организации на запрос субъекта персональных данных (далее – СПД), обрабатываемых Организацией состоит из двух частей: идентификационной и содержательной.

В идентификационную часть включаются сведения из соответствующего запроса СПД, а также фамилия и данные паспорта гражданина Российской Федерации – первые две цифры серии и последние четыре цифры номера (например, 45** **1234), для иных документов, удостоверяющих личность в соответствии с законодательством Российской Федерации, указываются последние четыре цифры номера.

Содержательная часть ответа сообщает о результате обращения в Организацию.

Формы ответов

1. Форма ответа на принятый и успешно обработанный запрос к Организации в случае, если Организация производит обработку персональных данных субъекта.

В ответ на Ваш запрос:
дата запроса: (дата получения запроса Организацией)
фамилия: (фамилия, указанная в запросе)
документ: (данные паспорта гражданина Российской Федерации – первые две цифры серии и последние четыре цифры номера (например, 45** **1234), для иных документов, удостоверяющих личность в соответствии с законодательством Российской Федерации, указываются последние четыре цифры номера)
Организация сообщает:
по состоянию на: (дата ответа Организации)
Организация подтверждает факт обработки персональных данных.
– указывается также цель такой обработки_____;
– способы обработки персональных данных, применяемые оператором _____;
– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ_____;
– перечень обрабатываемых персональных данных и источник их получения_____;
– сроки обработки персональных данных, в том числе сроки их хранения_____;
– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных_____.

2. Форма ответа на запрос СПД если сведения по данному СПД не найдены.

В ответ на Ваш запрос:
дата запроса: (дата получения запроса Организацией)
фамилия: (фамилия, указанная в запросе)
документ: (данные паспорта гражданина Российской Федерации – первые две цифры серии и последние четыре цифры номера (например, 45** **1234), для иных документов, удостоверяющих личность в соответствии с законодательством Российской Федерации, указываются последние четыре цифры номера)
Организация сообщает:
по состоянию на: (дата ответа Организации) обработка персональных данных Организацией указанного гражданина не производится.

3. Форма ответа на запрос СПД в случае если формат поступившего запроса не соответствует требованиям, установленным законодательством.

В ответ на Ваш запрос:

дата запроса: (дата получения запроса)

фамилия: (фамилия, указанная в запросе) (может отсутствовать, если из поступившего запроса невозможно определить значение данного поля)

документ: (данные паспорта гражданина Российской Федерации – первые две цифры серии и последние четыре цифры номера (например, 45** **1234), для иных документов, удостоверяющих личность в соответствии с законодательством Российской Федерации, указываются последние четыре цифры номера) (может отсутствовать, если из поступившего запроса невозможно определить значение данного поля)

Организация сообщает:

по состоянию на: (дата ответа Организации) неверный формат запроса.

Приложение 20

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания №2 от «30» сентября 2019 года.

Инструкция по уничтожению ПДн

Настоящая Инструкция разработана в соответствии с от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (далее – Закон № 152-ФЗ).

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

2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3. Субъект персональных данных вправе требовать от Организации уничтожения своих персональных данных в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

О предпринятых к уничтожению персональных данных мерах Организация обязана уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

4. В случае выявления неправомерных действий с персональными данными Организация в срок, не превышающий трех рабочих дней с даты такого выявления, обязана устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Организация в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, Организация обязана уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Организация обязана уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, – также указанный орган.

5. В случае достижения цели обработки персональных данных Организация обязана незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, – также указанный орган.

6. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Организация обязана прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Организацией и субъектом персональных данных. Об уничтожении персональных данных Организация обязана уведомить субъекта персональных данных.

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

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

9. Уничтожение ПДн и носителей ПДн производится комиссией, в состав которой входят работники/агенты Организации, осуществляющие обработку уничтожаемых ПДн, начальники подразделений, в которых обрабатываются уничтожаемые ПДн и носители ПДн и СА.

10. По результатам уничтожения персональных данных составляются Акты Приложений №№ 10, 13 к Положению.

Приложение 21

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПД СКПК «ДЕНЕЖНЫЙ ПОТОК», утвержденному протоколом Общего собрания № 2 от «30» сентября 2019 года.

Акт
об обезличивании в Организации персональных данных

Мы, нижеподписавшиеся _____
(должность, фамилия и инициалы)

_____

составили настоящий акт в том, что перечисленные в нем персональные данные подлежат обезличиванию

_____
(указать причину уничтожения персональных данных)
_____
_____

№. п/п	Персональные данные, подлежащие обезличиванию	Наименование документа, содержащего персональные данные	вид носителя персональных данных	количество экземпляров	Количество листов в 1 экз.	Порядок обезличивания персональных данных
1	2	3	4	5	6	7

Всего подлежит обезличиванию _____ персональных данных.
(прописью)

_____ экз.

"___"_____ 201_ г. Подписи:
1.
2.
3.

Документы перед уничтожением сверили с записями в акте и полностью уничтожили путем _____

"___"_____ 200_ г. Подписи:
1.
2.
3.