УТВЕРЖДАЮ

Директор ООО «СТАВМЕДКЛИНИКА»

_____ / А.Н.Айдемиров

«02»марта 2020 г.

М.П.

Приказ
ООО «СТАВМЕДКЛИНИКА»
От 02 марта 2020 года №4-од

ПОЛОЖЕНИЕ
о порядке организации и проведении работ по обработке и защите персональных данных, обрабатываемых в информационных системах персональных данных ООО «СТАВМЕДКЛИНИКА»

г. Ставрополь
2020 г.

1. Общие положения

1.1. Настоящее «Положение о порядке организации и проведении работ по обработке и защите персональных данных, обрабатываемых в информационных системах персональных данных ООО «СТАВМЕДКЛИНИКА» (далее – Положение) разработано на основании:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Налогового кодекса Российской Федерации;
- Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- других нормативно-правовых актов Российской Федерации.

1.2. Настоящим Положением определяется порядок обработки, т.е. действий (операций) с персональными данными (далее – ПДн), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн сотрудников и пациентов ООО «СТАВМЕДКЛИНИКА» с использованием средств автоматизации или без использования таких средств. Положение устанавливает требования по защите ПДн, принципы обработки ПДн в информационных системах персональных данных (далее – ИСПДн).

1.3. Целью настоящего Положения является обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты ПДн граждан.

1.4. Основные термины и определения, применяемые в настоящем Положении:

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

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

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

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

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

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

1.4.7. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

1.4.9. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4.10. Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

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

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

1.5. К субъектам персональных данных (далее – субъекты) относятся лица, ПДн которых переданы ООО «СТАВМЕДКЛИНИКА», (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для обработки (в том числе передачи).

1.6. ПДн 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 Управления.

1.7. Обработка ПДн субъекта без письменного его согласия не допускаются, если иное не определено законодательством РФ. ПДн относятся к категории конфиденциальной информации. Режим конфиденциальности ПДн снимается в случаях обезличивания или по истечении сроков хранения, если иное не определено Законодательством РФ.

1.8. Должностные лица ООО «СТАВМЕДКЛИНИКА», в обязанности которых входит обработка ПДн субъектов, обязаны обеспечить каждому субъекту возможность ознакомления со своими ПДн, если иное не предусмотрено законодательством РФ.

1.9. ПДн не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

1.10. Настоящее Положение и изменения к нему утверждаются директором ООО «СТАВМЕДКЛИНИКА», являются обязательными для исполнения всеми сотрудниками, имеющими доступ к ПДн субъектов ПДн.

2. Принципы обработки персональных данных

2.1. Обработка ПДн в ООО «СТАВМЕДКЛИНИКА» осуществляется на основе следующих принципов:

- законности и справедливости обработки ПДн;
- законности целей и способов обработки ПДн и добросовестности;
- соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Управления;
- соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн;
- достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

2.2. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.3. Субъект ПДн является собственником своих ПДн и самостоятельно решает вопрос передачи Учреждению своих ПДн.

2.4. Держателем ПДн является ООО «СТАВМЕДКЛИНИКА» которому субъект ПДн передает во владение свои ПДн. Управление выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

3. Понятие и состав персональных данных

3.1. Под ПДн субъектов понимается информация необходимая ООО «СТАВМЕДКЛИНИКА» для:

- исполнение требований трудового законодательства и трудового договора с сотрудником;
- оказание услуг пациентам ООО «СТАВМЕДКЛИНИКА»;
- ведение бухгалтерского, налогового и кадрового учета;

- передача персональных данных сотрудников в банковские организации для содействия в открытии банковских карт;
- начисления заработной платы сотрудникам.

3.2. К ПДн субъектов ПДн относятся следующие сведения:

- ФИО;
- паспортные данные;
- дата и место рождения;
- гражданство;
- данные о регистрации;
- сведения об образовании;
- сведения о воинском учете;
- место жительства;
- ИНН, СНИЛС, номер страхового полиса;
- номер телефона (домашний, сотовый);
- семейное положение;
- сведения о зарплате, налогах;
- лицевой счет.
- страховой медицинский полис обязательного (добровольного медицинского страхования 9для пациентов)

3.3. Документы, содержащие ПДн, являются конфиденциальными.

4. Получение, обработка и хранение персональных данных

4.1. Учреждение получает сведения о ПДн субъектов ПДн из следующих источников:

- паспорта или иного документа, удостоверяющего личность;
- анкет, заполняемых гражданами.

Субъект ПДн обязан предоставлять ООО «СТАВМЕДКЛИНИКА» достоверные сведения о себе. Учреждение имеет право проверять достоверность указанных сведений в порядке, не противоречащем законодательству Российской Федерации.

4.2. Обработка ПДн субъекта ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

4.3. При определении состава обрабатываемых ПДн субъектов ООО «СТАВМЕДКЛИНИКА» руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

4.4. ПДн субъекта ООО «СТАВМЕДКЛИНИКА» получает непосредственно от субъекта. Ответственный сотрудник принимает от субъекта материальные носители ПДн (документы, копии документов), сверяет копии документов с подлинниками.

4.5. Условием обработки ПДн субъекта ПДн является его письменное согласие. Письменное Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

Согласие на обработку ПДн может быть отозвано субъектом ПДн в соответствии с положением статьи 9 Федерального закона № 152 «О персональных данных».

4.6. Согласия субъекта на обработку его ПДн не требуется в следующих случаях:

- обработка ПДн 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;
- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- обработка ПДн 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 ПДн;
- обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;
- осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе;
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.7. Для обработки ПДн, содержащихся в согласии в письменной форме субъекта на обработку его ПДн, дополнительное согласие не требуется.

4.8. В случае недееспособности субъекта ПДн согласие на обработку его персональных данных в письменной форме дает его законный представитель.

В случае смерти субъекта согласие на обработку его ПДн при необходимости дает в письменной форме один из его наследников, если такое согласие не было дано субъектом ПДн при его жизни.

4.9. Защита ПДн субъекта от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральным законодательством Российской Федерации.

4.10. Субъекты ПДн и их представители должны быть ознакомлены под роспись с документами Учреждения, устанавливающими порядок обработки ПДн, а также об их правах и обязанностях в этой области.

4.11. Основным источником, содержащим ПДн граждан, является база данных 1С.

4.12. При обработке ПДн главный директор ООО «СТАВМЕДКЛИНИКА» вправе определять способы обработки, документирования, хранения и защиты ПДн на базе современных информационных технологий.

4.13. Перечень лиц, допущенных к обработке ПДн, определяется приказом директора ООО «СТАВМЕДКЛИНИКА».

4.14. Обработка ПДн, осуществляются уполномоченными работниками ООО «СТАВМЕДКЛИНИКА», определенными приказом директора, которые действуют на основании инструкций, предусматривающих выполнение комплекса мероприятий по обеспечению безопасности ПДн.

4.15. Ответственность за контроль соблюдения требований по обработке ПДн, контроль соблюдения прав и свобод субъектов ПДн возлагается на директора ООО «СТАВМЕДКЛИНИКА».

4.16. Помещения, в которых обрабатываются и хранятся ПДн субъектов, оборудуются надежными замками. Должно быть исключено бесконтрольное пребывание посторонних лиц в этих помещениях.

Для хранения ПДн используются специально оборудованные шкафы или сейфы, которые запираются на ключ.

Помещения, в которых обрабатываются и хранятся ПДн субъектов, в рабочее время при отсутствии в них работников должны быть закрыты.

Проведение уборки помещений, в которых хранятся ПДн, должно производиться в присутствии ответственных работников.

5. Права и обязанности сторон в области защиты персональных данных

5.1. Субъект персональных данных обязан:

- передать ООО «СТАВМЕДКЛИНИКА» комплекс достоверных, документированных ПДн.
- своевременно, в срок, не превышающий 5 (пяти) рабочих дней, сообщать ответственному лицу учреждения об изменении своих ПДн.

5.2. Субъект ПДн имеет право:

- на получение сведений об учреждении, о месте его нахождения, о наличии у ООО «СТАВМЕДКЛИНИКА» ПДн, относящихся к соответствующему субъекту ПДн, а также на ознакомление с такими ПДн, за исключением случаев, если предоставление ПДн нарушает конституционные права и свободы других лиц;
- на свободный бесплатный доступ к своим ПДн, включая право на получение копии любой записи, содержащей ПДн, за исключением случаев, предусмотренных федеральными законами;
- получать информацию, касающуюся обработки его ПДн, в том числе содержащую:
  1) подтверждение факта обработки ООО «СТАВМЕДКЛИНИКА»;
  2) правовые основания и цели обработки ПДн;
  3) цели и применяемые способы обработки ПДн, применяемые оператором;
  4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
  5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
  6) сроки обработки ПДн, в том числе сроки их хранения;
  7) порядок осуществления субъектом ПДн прав, предусмотренных настоящим Федеральным законом;
  8) сведения о том, какие юридические последствия для него может повлечь за собой обработка его ПДн;
- обжаловать в судебном порядке любые неправомерные действия или бездействие ООО «СТАВМЕДКЛИНИКА» при обработке и защите ПДн;
- требовать об извещении ООО «СТАВМЕДКЛИНИКА» всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- требовать от ООО «СТАВМЕДКЛИНИКА» исключения, исправления или уточнения своих персональных данных, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- при отказе оператора исключить или исправить ПДн субъекта заявить в письменной форме ООО «СТАВМЕДКЛИНИКА» о своем несогласии с соответствующим обоснованием такого несогласия, при отклонении оператором указанного обращения (несогласия), обжаловать

действия оператора в порядке, предусмотренном законодательством Российской Федерации.

Сведения о ПДн должны быть предоставлены субъекту в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

5.3. Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, не может быть принято на основании исключительно автоматизированной обработки его ПДн.

5.4. ООО «СТАВМЕДКЛИНИКА» обязано разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов.

5.5. ООО «СТАВМЕДКЛИНИКА» обязано рассмотреть возражение субъекта ПДн в течение 30 (тридцати) рабочих дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

5.6. Если обязанность предоставления ПДн субъектом установлена федеральным законом (включая налоговое, трудовое право), Роскомнадзор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить свои ПДн.

5.7. ООО «СТАВМЕДКЛИНИКА» обязано безвозмездно предоставить субъекту ПДн возможность ознакомления с ПДн, относящимися к нему, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие ПДн по предоставлении субъектом сведений, подтверждающих, что ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

5.8. ООО «СТАВМЕДКЛИНИКА» обязано сообщить в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа в установленные нормативно-правовыми актами Российской Федерации сроки.

5.9. В случае выявления недостоверных ПДн или неправомерных действий с ними, ООО «СТАВМЕДКЛИНИКА» обязано осуществить блокирование ПДн, относящихся к соответствующему субъекту, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности ПДн, обрабатываемых в ООО «СТАВМЕДКЛИНИКА», на основании соответствующих документов обязан уточнить ПДн в течение 7 (семи) рабочих дней со дня их получения и снять их блокирование.

5.10. В случае выявления неправомерных действий с ПДн, ООО «СТАВМЕДКЛИНИКА» в срок, не превышающий 3 (трех) рабочих дней с даты такого выявления, обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений, ООО «СТАВМЕДКЛИНИКА» в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерности действий с ПДн, обязано уничтожить ПДн. Об устранении допущенных нарушений или об уничтожении ПДн, ООО «СТАВМЕДКЛИНИКА» обязано уведомить субъекта ПДн или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн.

5.11. В случае достижения цели обработки ПДн ООО «СТАВМЕДКЛИНИКА» обязано незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий 30 (тридцати) рабочих дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

5.12. В случае отзыва субъектом согласия на обработку своих ПДн ООО «СТАВМЕДКЛИНИКА» обязано прекратить обработку ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн в срок, не превышающий 30 (тридцати) рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон и (или) федеральным законом. Об уничтожении ПДн оператор обязан уведомить субъекта ПДн.

В случае невозможности уничтожения ПДн в течение вышеуказанного срока ООО «СТАВМЕДКЛИНИКА» должно осуществить блокирование таких ПДн и обеспечить уничтожение ПДн в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

5.13. До начала обработки ПДн ООО «СТАВМЕДКЛИНИКА» обязано уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев установленных законодательством Российской Федерации.

5.14. Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации. Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес ООО «СТАВМЕДКЛИНИКА»;
- цель обработки ПДн;
- категории ПДн;
- категории субъектов, ПДн которых обрабатываются;
- правовое основание обработки ПДн;
- перечень действий с ПДн, общее описание используемых способов обработки ПДн;
- описание мер, применяемых ООО «СТАВМЕДКЛИНИКА» для обеспечения безопасности ПДн, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки ПДн, и их контактные сведения;
- дата начала обработки ПДн;
- срок или условие прекращения обработки ПДн;
- сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;
- сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.

6. Доступ к персональным данным субъекта и их передача

6.1. Внутренний доступ (доступ внутри ООО «СТАВМЕДКЛИНИКА») к ПДн субъектов имеют сотрудники подразделений ООО «СТАВМЕДКЛИНИКА», которым эти данные необходимы для выполнения должностных обязанностей.

После прекращения юридических отношений с субъектом ПДн документы, содержащие его ПДн, хранятся в ООО «СТАВМЕДКЛИНИКА» в течение сроков, установленных архивным и иным законодательством Российской Федерации.

6.2. Внешний доступ к ПДн субъектов имеют массовые потребители ПДн и контрольно-надзорные органы.

6.2.1. К числу массовых потребителей ПДн вне ООО «СТАВМЕДКЛИНИКА» относятся следующие государственные и негосударственные структуры:

- ПФР, УФНС и ФСС России;
- правоохранительные органы;
- органы прокуратуры, МВД и ФСБ России.

6.2.2. Контрольно-надзорные органы имеют доступ к информации исключительно в сфере своей компетенции.

6.3. Внешний доступ со стороны третьих лиц к ПДн субъекта осуществляется с его письменного согласия, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъекта или других лиц, и иных случаев, установленных законодательством.

6.4. ООО «СТАВМЕДКЛИНИКА» обязано сообщать ПДн субъекта по надлежаще оформленным запросам суда, прокуратуры иных правоохранительных органов.

6.6. ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта ПДн.

6.7. При передаче ПДн ООО «СТАВМЕДКЛИНИКА» должно соблюдать следующие требования:

- не сообщать ПДн субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в случаях, установленных федеральными законами;
- не сообщать ПДн субъекта в коммерческих целях без его письменного согласия;
- предупреждать лиц, получающих ПДн субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц

подтверждения того, что это правило соблюдено, за исключением случаев, когда обмен ПДн осуществляется в порядке, установленном федеральными законами;

- не запрашивать информацию о состоянии здоровья субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- разрешать доступ к ПДн, исключительно специально уполномоченным лицам (при этом указанные лица должны иметь право получать лишь те ПДн, которые необходимы для выполнения конкретных функций);
- в должностных инструкция уполномоченных лиц должны быть прописаны обязательства по неразглашению и выполнению требований нормативных документов по обработке и обеспечению безопасности персональных данных.

6.8. Передача ПДн от держателя или его представителей в другие учреждения и организации может допускаться только при наличии письменного согласия субъекта ПДн в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.9. Ответы на правомерные письменные запросы других учреждений и организаций даются с разрешения директора ООО «СТАВМЕДКЛИНИКА» в письменной форме, в том объеме, который позволяет не разглашать излишний объем ПДн.

6.10. Не допускается передача ПДн по открытым каналам связи, в том числе по телефону.

6.11. Сведения, передаваемые в письменной форме, должны иметь пометку о конфиденциальности. В сопроводительном письме к таким документам указывается, что в прилагаемых документах содержатся ПДн субъектов.

6.12. ООО «СТАВМЕДКЛИНИКА» не допускается осуществление трансграничной передачи персональных данных.

7. Защита персональных данных

7.1. Комплекс мер по защите ПДн направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности ПДн и обеспечивает безопасность информации в процессе деятельности ООО «СТАВМЕДКЛИНИКА».

7.2. ООО «СТАВМЕДКЛИНИКА» при обработке ПДн обязано принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИСПДн.

7.3. Мероприятия по защите ПДн определяются настоящим Положением, приказами, инструкциями и другими внутренними документами ООО «СТАВМЕДКЛИНИКА» .

7.4. Для защиты ПДн в ООО «СТАВМЕДКЛИНИКА» применяются следующие принципы и правила:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей ПДн;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно-методических документов по защите ПДн;
- распределение персональной ответственности между сотрудниками, участвующими в обработке ПДн, за выполнение требований по обеспечению безопасности ПДн.
- установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности ПДн при работе с конфиденциальными документами и базами данных;
- исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка ПДн и находится соответствующая вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа;
- воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн;
- ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся ПДн.
- создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией;
- резервирование защищаемых данных (создание резервных копий).

8. Допуск персонала к обработке ПДн

8.1. При допуске к обработке ПДн необходимо руководствоваться Приказом о допуске к обработке ПДн.

8.2. Перечни должностных лиц составляются и ведутся владельцами ИСПДн и процессов обработки ПДн, на основании данных о должностных лицах, допущенных к ПДн.

Доступ конкретных лиц к ПДн и ИСПДн осуществляется на основании служебных записок (заявок). Служебные записки на доступ учитываются и хранятся администратором информационной безопасности ИСПДн.

8.3. Конкретный регламент предоставления доступа определен в «Инструкции по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИСПДн».

9. Обучение персонала, участвующего в обработке ПДн

9.1. Должно проводиться регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн.

9.2. В общем случае, для различных категорий сотрудников форматы обучения должны отличаться.

Определены следующие форматы обучения:

- полные курсы (длительностью 5 дней и более);
- кратковременные курсы (длительностью от 1 до 3 дней);
- внешние и внутренние семинары;
- конференции;
- инструктажи.

9.2.1. Полные и кратковременные курсы, конференции, внешние семинары проводятся во внешних специализированных организациях для следующих категорий сотрудников:

- ответственный за обеспечение безопасности и обработки ПДн;
- администратор информационной безопасности ИСПДн.

9.2.2. Для обучения остальных категорий персонала, участвующих в процессах обработки ПДн, должны проводиться:

- внутренние семинары;
- инструктажи.

Внутренние семинары проводятся ответственным за обеспечение безопасности и обработки ПДн, администратором информационной безопасности ИСПДн, а также могут проводиться приглашенными специалистами или другими подготовленными лицами. На всех семинарах следует использовать презентации.

9.3. Обучение каждой категории сотрудников должно проводиться не реже одного раза в год.

Инструктажи проводятся в отношении отдельных лиц, по мере необходимости АИБ ИСПДн, ответственным за обеспечение безопасности и обработки ПДн.

При необходимости могут разрабатываться инструкции, описывающие особенности обработки ПДн в каждой ИСПДн, для отдельных категорий (групп) персонала.

Проведения инструктажей должно фиксироваться в «Журнале учета проведе-ния инструктажей по вопросам защиты информации».

9.4. Для проведения семинаров создаются учебные группы по структурным подразделениям. Состав группы не должен превышать 5-10 человек.

Инструкторы учебных групп должны в первый год, а в дальнейшем не реже 1 раза в 3 года проходить подготовку в специализированных учебно-методических центрах по вопросам защиты ПДн.

10. Организация работы с носителями ПДн

10.1. Для организации документооборота связанного с ПДн в ООО «СТАВМЕДКЛИНИКА» должны быть упорядочены и регламентированы следующие работы, связанные с ПДн:

- учет носителей, содержащих ПДн;
- обращение с носителями, содержащими ПДн;
- систематизация носителей, содержащих ПДн;
- хранение носителей, содержащих ПДн;
- подготовка носителей, содержащих ПДн для передачи их в архив;
- подготовка носителей, содержащих ПДн для их уничтожения;
- проверка наличия носителей, содержащих ПДн;
- распечатка ПДн.

Должны регламентироваться работы с ПДн в виде документов на следующих носителях:

- бумажных носителях;
- электронных съемных носителях;
- электронных несъемных носителях, используемых в технических средствах ИСПДн.

10.2. Порядок работ с носителями ПДн должен быть регламентирован в соответствующих внутренних нормативных документах.

11. Уничтожение ПДн

11.1. В соответствии с нормативными актами РФ ПДн должны быть уничтожены:

- по требованию субъекта ПДн, в определенных законодательством РФ случаях;
- при истечении срока хранения;
- в случае выявления неправомерных действий с ПДн и невозможности устранения допущенных нарушений;
- в случае достижения цели обработки ПДн;
- в случае утраты необходимости достижения цели обработки.

Контроль сроков хранения, целей обработки ПДн производится на основании допустимых сроков хранения и допустимых целей.

11.2. Решение об уничтожении ПДн, организацию и проведение уничтожения принимают и осуществляют владельцы ИСПДн и процессов обработки ПДн.

11.3. Порядок уничтожения ПДн должен быть регламентирован в нормативных документах ООО «СТАВМЕДКЛИНИКА».

Об уничтожении ПДн должен быть уведомлен субъект ПДн.

11.4. После проведенного уничтожения должен быть подготовлен акт об уничтожении ПДн. Форма акта приведена в Приложении Приложение № 1.

12. Защита от несанкционированного физического доступа к элементам ИСПДн

12.1. Мероприятия по физическому контролю доступа включают:

- контроль доступа на территорию;
- контроль доступа в помещения с оборудованием ИСПДн;
- контроль доступа к техническим средствам ИСПДн;
- контроль перемещений физических компонентов ИСПДн.

12.2. Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн должны иметь прочные входные двери с надежными замками. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников.

Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками.

12.3. Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие сотрудники), должно допускаться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

12.4. Расположение мониторов рабочих станций должно препятствовать их несанкционированному

просмотру со стороны других лиц, не являющихся пользователями ИСПДн.

12.5. В нерабочее время, по окончании рабочего дня двери помещений должны быть закрыты на замок.

12.6. При выносе устройств, хранящих ПДн, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

12.7. В отношении некоторых ИСПДн возможны дополнительные, либо более низкие требования по физической защите. Состав таких требований определяется по результатам разработки Модели угроз и нарушителя и ТЗ (СТЗ, ЧТЗ) на создание СЗПДн. Мероприятия по защите таких ИСПДн определяются эксплуатационной (проектной) документацией.

13. Резервирование ПДн

13.1. Резервирование ПДн должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

В регламенте процесса резервирования должны быть учтены следующие вопросы:

- порядок резервирования;
- ответственные за резервирование;
- порядок восстановления информации после аварий;
- порядок хранения резервных копий.

Резервированию должна подвергаться информация на серверах ИСПДн.

Резервирование должно осуществляться на магнитные ленты или другие носители информации с соответствующим уровнем надежности и долговечности.

13.2. Хранение резервных копий должно осуществляться в сейфах (запираемых шкафах, ящиках). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

13.3. Доступ к резервным копиям должен быть строго регламентирован.

13.4. Резервирование должно осуществляться в соответствии с инструкцией резервного копирования Учреждения.

14. Реагирование на нештатные ситуации

14.1. Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн, в Учреждении должны быть регламентированы следующие вопросы:

- порядок определения нештатной ситуации;
- порядок оповещения сотрудников при возникновении различных нештатных ситуаций;
- порядок действий персонала в нештатных ситуациях.

В Учреждении должны проводиться расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями.

В рамках данного процесса должны решаться следующие задачи:

- расследование инцидентов, связанных с безопасностью ПДн;
- ликвидация последствий инцидентов связанных с безопасностью ПДн;
- принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

Реагирование на нештатные ситуации должно производиться в соответствии с «Инструкцией по действиям пользователей ИСПДн в нештатных ситуациях».

15. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

15.1. Персональная ответственность является одним из главных требований к организации функционирования СЗПДн и обязательным условием обеспечения эффективности функционирования данной системы.

15.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

15.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или

уголовную ответственность в соответствии с федеральными законами.

15.4. Каждый сотрудник ООО «СТАВМЕДКЛИНИКА», получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность полученной информации.

15.5. Должностные лица, в обязанность которых входит обработка ПДн, обязаны обеспечить каждому субъекту ПДн, возможность ознакомления с документами и материалами, если иное не предусмотрено законом.

Неправомерный отказ в предоставлении собранных в установленном порядке ПДн, либо несвоевременное их предоставление в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного наказания в порядке, установленном Кодексом Российской Федерации об административных правонарушениях.

15.6. В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, содержащую ПДн, обязаны возместить причиненные убытки; такая же обязанность возлагается и на работников, не обладающих правом доступа к ПДн.

15.7. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения влечет наложение наказания в порядке, предусмотренном Уголовным кодексом Российской Федерации.

15.8. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию ПДн может быть установлена в судебном порядке.

16. Обработка персональных данных без использования средств автоматизации

Особенности обработки персональных данных, осуществляемой без использования средств автоматизации:

16.1. 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, а также если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

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

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

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

16.3. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

16.4. При составлении типовых форм необходимо, чтобы каждый субъект ПДн, чьи персональные данные указаны в документе, имел возможность ознакомиться со своими персональными данными, содержащими в документе, не нарушая прав и законных интересов иных лиц.

Приложение № 1
к «Положению
о порядке организации и проведении работ
по обработке и защите персональных
данных, обрабатываемых в ООО
«СТАВМЕДКЛИНИКА»

Форма акта уничтожения документов, содержащих персональные данные

У Т В Е Р Ж Д А Ю
Директор
ООО «СТАВМЕДКЛИНИКА»
_____ ___/ А.Н.Айдемиров
«____» _____ 2020 г.

АКТ
уничтожения документов, содержащих персональные данные

«___»_____20__ г. № _____

Комиссия в составе:
председатель –
_____;
и членов комиссии –
_____;
_____;
_____,
произвела отбор для уничтожения следующие документы, содержащие персональные данные:

№ п/п	Наименование документа	Регистрационный номер документа	Дата регистрации	Номер экз.	Количество листов документа/ приложения
1	2	3	4	5	6

Всего подлежит уничтожению _____ (_____) наименований
(цифрами) (прописью)
документов. Записи акта с регистрационными данными сверены.

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

После утверждения акта, перед уничтожением отобранные документы с записями в акте сверили и полностью уничтожили путем измельчения в бумагорезательной машине.

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