ПОЛОЖЕНИЕ

по обработке персональных данных в ООО «АвиценнаДент»

1 Общие положения

1.1. Данное «Положение по обработки персональных данных в ООО «АвиценнаДент» (далее – «Положение») определяют правила обработки персональных данных, разработаны в соответствии с Конституцией РФ, Федеральным законом от 30.12.2001 г. № 197-ФЗ «Трудовой кодекс РФ», Федеральными законами от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21 марта 2012 г. N 211 «Об утверждении перечня 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», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Федеральным законом от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Указом Президента Российской Федерации от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», Положением «О порядке организации и проведения работ по защите конфиденциальной информации в ООО «АвиценнаДент»» в целях обеспечения безопасности персональных данных сотрудников, а также граждан, чьи персональные данные обрабатываются сотрудниками ООО «АвиценнаДент».

1.2. Положение определяют порядок обработки в ООО «АвиценнаДент» персональных данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

2 Термины и определения

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

2) **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;

3) **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;

4) **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

5) **Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) **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;

9) **Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) **Информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) **Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3 Категории субъектов, персональные данные которых обрабатываются в ООО «АвиценнаДент»

ООО «АвиценнаДент» обрабатывает персональные данные, которые может получить от следующих субъектов персональных данных:

граждан, состоящих с ООО «АвиценнаДент» в отношениях, регулируемых трудовым законодательством, законодательством о государственной гражданской службе;

граждан, являющихся претендентами на замещение должностей в ООО «АвиценнаДент»;

граждан, обращающихся в ООО «АвиценнаДент».

4 Порядок обработки персональных данных граждан, состоящих с ООО «АвиценнаДент» в отношениях, регулируемых трудовым законодательством

4.1 Цели и порядок обработки персональных данных граждан, состоящих с ООО «АвиценнаДент» в отношениях, регулируемых трудовым законодательством

Обработка персональных данных граждан указанных категорий ведется в соответствии с Федеральным законом от 30.12.2001 г. № 197-ФЗ «Трудовой кодекс РФ», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» ст.6 ч.1 п.2., Федеральным законом от 21.11.1996 г. № 129 «О бухгалтерском учете», Федеральным законом от 31.07.1998 г. № 146-ФЗ «Налоговый кодекс РФ» часть первая.

Обработка персональных данных граждан, состоящих с ООО «АвиценнаДент» в отношениях, регулируемых трудовым законодательством ведется с целью установления гарантий трудовых прав и свобод граждан, создание благоприятных условий труда, защиты прав и интересов сотрудников, установления режима обеспечения продвижения сотрудников по иерархии служебной деятельности.

Основными целями обработки персональных данных являются создание необходимых правовых условий для достижения оптимального согласования интересов сторон трудовых отношений, а также правовое регулирование трудовых отношений и иных непосредственно связанных с ними отношений по:

- организации труда и управлению трудом;
- трудоустройству у данного работодателя;
- профессиональной подготовке, переподготовке и повышению квалификации сотрудников ООО «АвиценнаДент»;
- участию сотрудников в установлении условий труда и применении трудового законодательства в предусмотренных законом случаях;
- материальной ответственности работодателей и сотрудников;
- разрешению трудовых споров;
- регулирование отношений по установлению, введению и взиманию налогов и сборов;
- обеспечению информацией об использовании материальных, трудовых и финансовых ресурсов в соответствии с утвержденными нормами, нормативами и сметами;
- обязательному социальному страхованию в случаях, предусмотренных федеральными законами.

Содержание персональных данных сотрудников, обрабатываемых в данных целях представляет собой сведения паспортных данных, сведения о трудовой деятельности, а так же дополнительные сведения, устанавливаемые федеральными законами и другими нормативными актами.

Обработка персональных данных ведется на основании заключаемого с этим лицом трудового договора с обязательным соблюдением конфиденциальности полученных персональных данных. Обработка персональных данных сотрудников осуществляется в соответствии со ст. 6 ч.1 п.2 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

ООО «АвиценнаДент» получает персональные данные сотрудников у них самих. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие на их получение. Персональные данные сотрудника могут быть получены ООО «АвиценнаДент» от лица, не являющегося субъектом персональных данных, при условии предоставления подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Сотрудник имеет право на получение информации, касающейся обработки его персональных данных, указанной в ст.14. часть 7 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» на основании запроса, составленному в соответствии со ст.14 часть 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Если предоставление персональных данных является обязательным в соответствии с федеральным законом, руководство ООО «АвиценнаДент» обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

Если персональные данные получены не от субъекта персональных данных, ООО «АвиценнаДент», за исключением случаев, предусмотренных ст.18 частью 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», до начала обработки таких персональных данных обязан предоставить сотруднику следующую информацию:

1) наименование и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

Персональные данные хранятся:

- в электронном виде (на серверах, персональных компьютерах, а также на сменных магнитных, оптических и других цифровых носителях);
- на бумажных носителях, в том числе в личных делах сотрудников, специально оборудованных шкафах и сейфах, обеспечивающих защиту от несанкционированного доступа.

При передаче персональных данных сотрудника необходимо соблюдать следующие требования:

- не сообщать персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в других случаях, предусмотренных Трудовым кодексом или иными федеральными законами;
- не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные сотрудника, 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. Лица, получающие персональные данные сотрудника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными сотрудников в порядке, установленном Трудовым кодексом и иными федеральными законами;
- осуществлять передачу персональных данных сотрудника в пределах организации в соответствии с настоящим Положением, с которым сотрудник должен быть ознакомлен под роспись;

- разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции;
- передавать персональные данные сотрудника представителям сотрудников в порядке, установленном Трудовым кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными сотрудника, которые необходимы для выполнения указанными представителями их функций.
- передача персональных данных сотрудников негосударственному пенсионному фонду и страховой компании в целях выполнения в отношении сотрудников условий о социальном обеспечении, а также банковским организациям с целью зачисления денежных средств осуществляется в соответствии с заключенными с этими организациями договорами и соглашениями о конфиденциальности (дополнительными соглашениями) при наличии письменного согласия сотрудников.

Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Не допускается обработка избыточных персональных данных.

Перечень должностей сотрудников, допущенных к персональным данным, утверждается приказом руководителя ООО «АвиценнаДент». Данные лица осуществляют обработку, включая сбор, накопление, систематизацию, уточнение, передачу персональных данных сотрудников в объёмах и целях, предусмотренных законодательством Российской Федерации и локальными нормативными актами ООО «АвиценнаДент», а также обеспечивают их защиту от неправомерного использования, утраты и несанкционированного уничтожения.

Защита персональных данных сотрудников от неправомерного их использования или утраты обеспечивается в ООО «АвиценнаДент» за счёт собственных средств в порядке, установленном Трудовым кодексом РФ и иными федеральными законами.

4.2 Ведение личных дел сотрудников ООО «АвиценнаДент»

4.2.1. Персональные данные и иные сведения, связанные с приёмом на работу, трудовой деятельностью и увольнением, вносятся в личное дело сотрудника ООО «АвиценнаДент» в связи с трудовыми отношениями. Личные дела сотрудников ведутся отделом кадров ООО «АвиценнаДент».

4.2.2. Совокупность персональных данных, внесенных в личные дела сотрудников, и иные сведения, содержащиеся в личных делах сотрудников, относятся к сведениям конфиденциального характера. На личное дело сотрудника ставится гриф «Для служебного пользования», на документы, хранящиеся в личном деле, гриф не проставляется.

4.2.2.1 К личному делу сотрудников ООО «АвиценнаДент» приобщаются:

- письменное заявление о приеме на работу (если таковое имеется);
- собственноручно заполненный и подписанный сотрудником личный листок по учету кадров установленной формы с приложением фотографии;
- копия паспорта;
- копия трудовой книжки;
- копия свидетельства о государственной регистрации актов гражданского состояния;
- копия документов о профессиональном образовании, персональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);
- копии решений о награждении государственными наградами, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются);
- копия приказа о приеме на работу;
- экземпляр трудового договора, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в трудовой договор;

- копии приказов о переводе сотрудников на другую постоянную работу, о переводе на другую работу временно;
- копии приказов о расторжении трудового договора;
- аттестационный лист сотрудника, прошедшего аттестацию;
- копии документов о присвоении сотруднику квалификационного разряда;
- копии приказов о поощрении сотрудника, а также о применении к нему дисциплинарного взыскания до его снятия или отмены;
- документы, связанные с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности связано с использованием таких сведений;
- копия страхового свидетельства обязательного пенсионного страхования.

4.2.4. В личное дело сотрудника вносятся также письменные объяснения сотрудника, если такие объяснения даны им после ознакомления с документами своего личного дела.

4.2.5. Документы, приобщенные к личному делу сотрудника, брошюруются, страницы нумеруются, к личному делу прилагается опись.

4.2.6. В обязанности сотрудника, осуществляющего ведение личных дел сотрудников, входит:

а) формирование и обеспечение сохранности личных дел сотрудников;

б) обеспечение конфиденциальности сведений, содержащихся в личных делах сотрудников, в соответствии с законодательством Российской Федерации и внутренними документами ООО «АвиценнаДент»;

в) ознакомление сотрудника с документами своего личного дела во всех случаях, предусмотренных законодательством Российской Федерации.

4.2.7. Личные дела уволенных сотрудников хранятся в отделе кадров ООО «АвиценнаДент» в течение двух лет со дня увольнения, после чего передаются в архив.

5 Порядок обработки персональных данных граждан, являющихся претендентами на замещение должностей в ООО «АвиценнаДент»

Обработка персональных данных ведется в соответствии с Федеральным законом от 30.12.2001 г. № 197-ФЗ «Трудовой кодекс РФ», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Целью обработки персональных данных граждан, являющихся претендентами на замещение должностей в ООО «АвиценнаДент» является установления факта возможности приема граждан на работу в ООО «АвиценнаДент».

Содержание персональных данных, обрабатываемых в этих целях, определяется сведениями, необходимыми для получения необходимой и достоверной информации о квалификации и личностных качествах претендента на вакантную должность в ООО «АвиценнаДент» в соответствии с действующим законодательством.

ООО «АвиценнаДент» получает персональные данные граждан, являющихся претендентами на замещение вакантных должностей у них самих.

Гражданин имеет право на получение информации, касающейся обработки его персональных данных, указанной в ст.14. часть 7 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» на основании запроса, составленному в соответствии со ст.14 часть 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Если предоставление персональных данных является обязательным в соответствии с федеральным законом, руководство ООО «АвиценнаДент» обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

Если персональные данные получены не от субъекта персональных данных, ООО «АвиценнаДент», за исключением случаев, предусмотренных ст.18 частью 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», до начала обработки таких персональных данных обязан предоставить сотруднику следующую информацию:

1) наименование и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

Персональные данные хранятся:

- в электронном виде (на серверах, персональных компьютерах, а также на сменных магнитных, оптических и других цифровых носителях);
- на бумажных носителях в специально оборудованных шкафах и сейфах, обеспечивающих защиту от несанкционированного доступа.

При передаче персональных данных граждан, являющихся претендентами на замещение вакантных должностей необходимо соблюдать следующие требования:

- не сообщать персональные данные граждан третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в других случаях, предусмотренных Трудовым кодексом или иными федеральными законами;
- не сообщать персональные данные гражданина в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные гражданина, 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. Лица, получающие персональные данные гражданина, обязаны соблюдать режим секретности (конфиденциальности);
- осуществлять передачу персональных данных гражданина в пределах организации в соответствии с настоящим Положением;
- разрешать доступ к персональным данным граждан, являющихся претендентами на замещение вакантных должностей только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья граждан, являющихся претендентами на замещение вакантных должностей, за исключением тех сведений, которые относятся к вопросу о возможности выполнения ими трудовой функции на рассматриваемой должности.

Не допускается обработка избыточных персональных данных.

6 Порядок обработки персональных данных граждан, обращающихся в ООО «АвиценнаДент».

Обработка персональных данных граждан указанных категорий ведется в соответствии с Конституцией РФ, Федеральными законами от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Положением «О порядке организации и проведения работ по защите конфиденциальной информации в ООО «АвиценнаДент».

Обработка персональных данных граждан, обращающихся в ООО «АвиценнаДент» ведется штатными сотрудниками.

Обработка персональных данных субъектов персональных данных осуществляется исключительно в целях охраны их жизни и здоровья субъекта, а также для обеспечения соблюдения законов и иных нормативно-правовых актов, контроля объема и качества выполняемой работы субъекта.

Все персональные данные предоставляются субъектом персональных данных соответственно в процессе лечения и обследования или трудовой деятельности.

ООО «АвиценнаДент» информирует субъекта о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента от дачи письменного согласия на их получение. Подтверждением информированности субъекта служит его письменное согласие на обработку персональных данных.

2.4 ООО «АвиценнаДент» информирует Общий единый источник персональных данных (общедоступный источник) для обработки персональных данных в целях защиты жизни, здоровья и иных жизненно важных интересов субъектов. В связи с этим доступ ООО «АвиценнаДент» к персональным данным на всех этапах их обработки неограниченному кругу лиц возможен только при получении письменного согласия субъекта персональных данных на их обработку.

2.5 Согласия на обработку и работу с персональными данными субъекта не требуется при:

-обработке персональных данных для защиты жизни, здоровья или иных жизненно важных интересов субъекта, если получение его согласия невозможно, а так же иных случаях предусмотренных действующим законодательством РФ.

7 Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

7.1 Обязанности по уточнению, блокированию и уничтожению персональных данных

7.1.1. 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 необходимо осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения.

7.1.2. 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 необходимо осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

7.1.3. В случае подтверждения факта неточности персональных данных необходимо на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.1.4. В случае достижения цели обработки персональных данных необходимо прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, является субъект персональных данных.

7.1.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных необходимо прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные 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.

7.1.6. 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.

7.1.7. Для уничтожения персональных данных, Приказом руководителя ООО «АвиценнаДент» назначается комиссия по уничтожению персональных данных. Уничтожение персональных данных оформляется актом.

7.1.8. Места хранения материальных носителей персональных данных утверждаются Приказом руководителя ООО «АвиценнаДент».

7.1.9. В ООО «АвиценнаДент» из числа сотрудников назначается ответственный за организацию обработки персональных данных, который обязан:

знать законодательство Российской Федерации и нормативные документы ООО «АвиценнаДент» в сфере обеспечения безопасности персональных данных;

осуществлять внутренний контроль за соблюдением ООО «АвиценнаДент» и его сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

доводить до сведения сотрудников ООО «АвиценнаДент» положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

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.

7.2. Права сотрудников ООО «АвиценнаДент» и граждан по обеспечению безопасности их персональных данных

Сотрудники и граждане имеют право на:

- полную информацию об их персональных данных и обработке этих данных;
- свободный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового Кодекса РФ или иного федерального закона;
- дополнение своих персональных данных оценочного характера заявлением, выражающим собственную точку зрения сотрудника;
- требование об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведённых в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия при обработке и защите его персональных данных.

7.3 Порядок хранения материальных носителей персональных данных

7.3.1. Основные принципы хранения отдельных материальных носителей персональных данных:

при фиксации персональных данных на материальных носителях не допускать фиксацию на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы;

для каждой категории персональных данных использовать отдельный материальный носитель;

материальные носители, содержащие персональные данные, обработка которых осуществляется в различных целях, хранить раздельно (в отдельных шкафах (сейфах), или на отдельных полках);

при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

7.3.2. Хранение отдельных материальных носителей персональных данных осуществляется на основании соответствующего приказа.

В приказе определяются:

места (номера комнат, шкафы (сейфы)), предназначенные для хранения материальных носителей персональных данных;

перечень работников (ФИО, должность), ответственных за реализацию принципов и требований по обеспечению безопасности носителей персональных данных;

требования по обеспечению безопасности персональных данных при хранении материальных носителей:

- порядок учёта материальных носителей;
- порядок доступа к носителям, получения носителей, работы с ними и порядок сдачи носителей на хранение;
- лицо (ФИО, должность), ответственное за хранение материальных
- носителей;
- лицо (ФИО, должность), ответственное за учёт материальных носителей;

порядок контроля выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных:

- лицо (ФИО, должность), ответственное за контроль выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных;
- обязанности лица (ФИО, должность), ответственного за контроль выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных.

7.4. Организация доступа к персональным данным

Система доступа к персональным данным представляет собой совокупность норм и правил, определяющих, кто из руководителей организации, кому из граждан и сотрудников и с какими категориями документов может давать разрешение на ознакомление.

Система доступа должна отвечать следующим требованиям:

- доступ к конфиденциальным документам может предоставляться сотрудникам, письменно оформившим с организацией отношения о неразглашении ставших им известными конфиденциальных сведений. Письменное оформление отношений о неразглашении конфиденциальной информации (соблюдения режима конфиденциальности) является обязательным условием для доступа исполнителей к документам;
- доступ к конфиденциальным документам должен быть обоснованным, т.е. базироваться на служебной необходимости ознакомления с конкретным документов именно данного исполнителя;
- система доступа должна давать возможность обеспечивать исполнителей всеми необходимыми им в силу служебных обязанностей документами, но только теми, которые действительно необходимы для выполнения конкретного вида работ;
- доступ к документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению уполномоченного на то должностного лица. При этом соответствующее должностное лицо может давать разрешение на ознакомление с документами только входящими в сферу его деятельности и только установленному кругу лиц;
- доступ должен оформляться письменно по каждому конкретному конфиденциальному документу. При необходимости ознакомления исполнителя только с частью документа в разрешении на ознакомление должны быть указаны разделы (пункты или страницы), с которыми можно знакомить исполнителя.

Доступ сотрудников организации к конфиденциальной информации осуществляется на добровольной основе. Эти отношения устанавливаются при приеме гражданина на работу или уже в ходе трудовых отношений. При этом необходимо выполнить следующие условия:

- ознакомить сотрудника под роспись с перечнем конфиденциальной информации;
- ознакомить сотрудника под роспись с установленным в организации режимом по охране конфиденциальности и с мерами ответственности за его нарушение;

- создать сотруднику необходимые условия для соблюдения им установленного режима по охране конфиденциальности.

Доступ к персональным данным разрешается только лицам, определенным в порядке, установленным настоящим Положением. При этом указанные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций, и в целях, для которых они сообщены.

Со стороны сотрудника предполагается принятие следующих обязательств:

- по соблюдению установленного в организации режима по охране конфиденциальности информации;
- о неразглашении конфиденциальной информации, ставшей ему известной в период выполнения трудовых отношений, после прекращения трудового договора в течение срока, предусмотренного в специальном соглашении или в течение трех лет, если такое соглашение на заключалось, и не использовании этой информации в личных целях;
- о возмещении причиненного ущерба, если сотрудник виновен в разглашении конфиденциальной информации, ставшей ему известной в связи с выполнением им трудовых обязанностей (в том числе после прекращения трудового договора);
- о возврате при прекращении или расторжении трудового договора всех имеющихся у сотрудника материальных носителей конфиденциальной информации.

Руководитель ООО «АвиценнаДент»:

- несет ответственность за организацию защиты персональных данных в организации;
- закрепляет за сотрудниками, допущенными к обработке персональных данных, конкретные массивы носителей с персональными данными, которые необходимы для выполнения возложенных на них функций;
- осуществляет внутренний контроль за соблюдением сотрудниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводит до сведения сотрудников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

С сотрудником, допущенным к персональным данным, заключается соглашение о допуске к конфиденциальной информации в установленном порядке. Соглашение от имени ООО «АвиценнаДент» подписывается руководителем ООО «АвиценнаДент».

Сведения о работающем (работавшем) сотруднике могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии согласия сотрудника на предоставление данных.

Доступ представителей государственных органов к персональным данным регламентируется законодательством Российской Федерации. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника. В случае развода бывшая супруга (супруг) имеет право обратиться в ООО «АвиценнаДент» с письменным запросом о размере заработной платы сотрудника без его согласия.

7.5 Обязанности лиц, допущенных к обработке персональных данных сотрудника

Лица, допущенные к работе с персональными данными обязаны:

знать законодательство Российской Федерации и нормативные документы ООО «АвиценнаДент» в части обеспечения безопасности персональных данных;

обеспечивать сохранность закрепленного массива носителей с персональными данными, исключать возможность ознакомления с ними других лиц;

докладывать своему непосредственному руководителю обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях;

ознакомиться под роспись с настоящим Положением, а также о правах, обязанностях, ответственности в области защиты персональных данных.

7.6 Правила рассмотрения запросов субъектов персональных данных или их представителей

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

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

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.

Все документы, поступающие от субъектов персональных данных, подлежат регистрации по журналу учета обращений субъектов персональных данных о выполнении их законных прав (См. Приложение 2).

На самом документе в правом нижнем углу первого листа документа проставляется отметка о поступлении, которая содержит входящий номер, присвоенный документу, дату поступления, количество листов.

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

- 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;
- 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;

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- 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.

ООО «АвиценнаДент» обязан сообщить 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.

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 ООО «АвиценнаДент» обязан дать в письменной форме мотивированный ответ, 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.

ООО «АвиценнаДент» 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. ООО «АвиценнаДент» 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.

ООО «АвиценнаДент» 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.

8 Меры по обеспечению безопасности персональных данных в ООО «АвиценнаДент»

В ООО «АвиценнаДент» должны быть приняты необходимые правовые, организационные и технические меры 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 в соответствии со статьей 19 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

8.1. Организационные и технические методы защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

а) Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

б) Действующими нормативными документами ФСТЭК России:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ от 13 февраля 2008 г. № 55 «Об утверждении порядка проведения классификации информационных систем персональных данных».

в) Действующими нормативными документами ФСБ России:

- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;
- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

г) Действующими документами Роскомнадзора:

- Приказ от 17 июля 2008 г. № 08 «Об утверждении образца формы уведомления об обработке персональных данных»
- Приказ от 1 декабря 2009 г. № 630 «Об утверждении административного регламента проведения проверок федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных»
- Приказ от 30 января 2010 г. № 18 «Об утверждении административного регламента федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции ведения реестра операторов, осуществляющих обработку персональных данных».

д) Настоящим Положением, Положением о порядке организации и проведения работ по защите конфиденциальной информации в ООО «АвиценнаДент» и другими локальными актами ООО «АвиценнаДент».

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии со Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утверждёнными приказом Гостехкомиссии России от 30 августа 2002 года № 282.

8.2. Приказом руководителя ООО «АвиценнаДент» определяется:

ответственный за организацию обработки персональных данных;
перечень автоматизированных систем, в которых обрабатываются персональных данные;
перечень сотрудников (должностей сотрудников), допущенных к персональным данным, и объём персональных данных, к которым они допускаются;
перечень персональных данных, обрабатываемый в информационной системе персональных данных.

8.3. С целью определения угроз безопасности персональных данных при обработке в информационных системах ООО «АвиценнаДент» должна быть проведена их классификация.

8.4. Должны быть разработаны модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, которые утверждаются руководителем ООО «АвиценнаДент».

8.5. В соответствии с классом информационной системы и моделью угроз безопасности персональных данных должны быть приняты меры в части технической защиты конфиденциальной информации. Информационные системы до начала обработки персональных данных должны пройти процедуру оценки эффективности принятых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

8.6. В информационных системах персональных данных должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.

8.7. В информационных системах персональных данных должны быть предусмотрены меры для предотвращения внедрения вредоносных программ (программ-вирусов) и программных закладок.

8.8. При взаимодействии информационных систем персональных данных с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования), должны применяться следующие методы и способы защиты информации от несанкционированного доступа:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации граждан;
- использование средств антивирусной защиты.

8.9. Должны быть проведены мероприятия по оценке эффективности принимаемых мер по обеспечению безопасности персональных данных. Должен проводиться контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

8.10. До начала обработки (в процессе обработки при наличии изменений) персональных данных направить в уполномоченный орган по защите прав субъектов персональных данных:

- уведомление о своем намерении осуществлять обработку персональных данных;
- фамилию, имя, отчество физического лица, ответственного за организацию обработки персональных данных, и номера его контактных телефонов, почтовые адреса и адреса электронной почты;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.