

ПРИКАЗ

01.12.2017 г

№ 24

г. Тюмень

Об утверждении формы согласия на обработку персональных данных, об утверждении правил конфиденциальности, сбора информации с использованием Интернет-ресурса

Во исполнение требований Федерального закона от 26.12.2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», в соответствии с административным регламентом исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, утвержденным приказом Минкомсвязи от 14.11.2011 №312

п р и к а з ы в а ю:

1. Утвердить форму согласия гражданина на обработку, хранение и использование персональных данных при оформлении записи на прием, консультацию ко врачу на сайте медицинской организации (Приложение № 1).

2. Утвердить Правила конфиденциальности персональных данных граждан, поступающих по средствам оформления записи на прием, консультацию ко врачу на сайте медицинской организации (Приложение № 2).

Директор



О.В. Кузина

СОГЛАСИЕ
на обработку, хранение и использование персональных данных при оформлении
записи на прием, консультацию ко врачу
на сайте медицинской организации

Настоящим, я (ФИО Лица), даю свое согласие ООО «Тюмень «Доктор ОСТ», г. Тюмень, ул. Мельникайте, д.138а/1 (далее – Клиника) на обработку своих персональных данных, указанных при оформлении заявки на сайте Компании для обработки моей записи на прием ко врачу, на консультацию ко врачу или любого другого способа обращения в Клинику (далее Запись), и связи со мной в рамках обработки моей Записи, а также иных сопряженных с этим целей в рамках действующего законодательства РФ и технических возможностей Клиники.

Обработка персональных данных Лица может осуществляться с помощью средств автоматизации и/или без использования средств автоматизации в соответствии с действующим законодательством РФ и положениями Клиники. Настоящее согласие Лица на обработку его/ее персональных данных, указанных при оформлении Записи на сайте Клиники, направляемых (заполненных) с использованием настоящего сайта, действует с момента оформления Записи на сайте Клиники до момента его отзыва. Согласие на обработку персональных данных, указанных при оформлении Записи на сайте Клиники, направляемых (заполненных) с использованием настоящего сайта, может быть отозвано Лицом при подаче письменного заявления (отзыва) в Клинику. Обработка персональных данных Лица прекращается в течение 2 месяцев с момента получения Клиникой письменного заявления (отзыва) Лица и/или в случае достижения цели обработки и уничтожается в срок и на условиях, установленных законом, если не предусмотрено иное. Обезличенные персональные данные Лица могут использоваться Клиникой в статистических (и иных исследовательских целях) после получения заявления (отзыва) согласия, а также после достижения целей, для которых настоящее согласие было получено.

Данный сайт позволяет ООО «Тюмень «Доктор ОСТ» получать информацию, содержащую персональные данные Лица, а именно фамилия имя отчество, контактный телефон, адрес электронной почты, а также другие персональные данные, которые могут использоваться для идентификации Лица («Ваши персональные данные»), в случае, если Лицо добровольно предоставляет их Клинике.

Лицо даёт согласие ООО «Тюмень «Доктор ОСТ» на обработку своих персональных данных, а именно: фамилия имя отчество, контактный телефон, адрес электронной почты, а также всех персональных данных, которые необходимы для связи с Лицом и оформление договора на оказание медицинских услуг.

В целях исполнения обязательств по договору Лицо предоставляет ООО «Тюмень «Доктор ОСТ» право осуществлять любые действия (операции) со своими персональными данными без ограничения: сбор, запись, учет, систематизацию, хранение, уточнение (обновление, изменение), извлечение, накопление, обезличивание, блокирование, удаление, уничтожение; использование в статистических целях, в целях проведения анализа, в целях информирования Лица (с передачей по SMS или электронной почтой) о продуктах и услугах Клиники, а также осуществлять любые иные действия с учетом действующего законодательства.

Правила конфиденциальности

Любая информация, передаваемая Лицом в связи с посещением сайта (Информация, которая не является персональными данными Лица и не может использоваться для идентификации Лица) может включаться в базы данных, которые принадлежат ООО «Тюмень «Доктор ОСТ» или их представителям. ООО «Тюмень «Доктор ОСТ» сохраняет все права на эти базы данных и информацию, которая в них хранится. Иная информация, которую мы собираем, может включать Ваш IP-адрес и прочую информацию, собираемую посредством cookie-файлов (см. ниже).

Данный сайт может использовать технологию, известную как cookie-файл. Cookie-файл - это сообщение, которое веб-сервер высылает на компьютер Лица, когда Лицо заходит на сайт. При повторном посещении, наш сайт проверит, имеется ли на компьютере Лица один из наших cookie-файлов. Наши cookie-файлы увеличивают функциональность сайта и помогают нам более точно анализировать, как используется сайт.

Данный сайт использует адреса Интернет-протокола (IP). IP-адрес - это номер, присваиваемый компьютеру Интернет-провайдером для доступа к Интернету. Обычно IP-адрес изменяется всякий раз, когда вы входите в Интернет (это "динамичный" адрес). Тем не менее, если используется высокоскоростное соединение, в зависимости от обстоятельств, возможно, что IP-адрес или даже cookie-файл, который мы используем, содержит идентифицируемую информацию. Это происходит потому, что при некоторых видах высокоскоростного соединения Ваш IP-адрес не изменяется ("статичен") и может ассоциироваться с компьютером Лица. Мы используем IP-адрес Лица для сообщения общей информации по использованию сайта, а также для его доработки.

Данный сайт использует технологию для определения местоположения Лица.

Лицо обязано покинуть данный сайт, если не хочет, чтобы вышеперечисленные данные (cookie, данные об IP-адресе и местоположении) обрабатывались.

Данный сайт не предназначен для лиц моложе 18 лет. Мы не собираем персональные данные лиц, которые по имеющейся у нас информации не достигли 18-летнего возраста. На данном сайте, где собирается информация, используется стандартное шифрование протокола защиты информации (SSL). Тем не менее, чтобы воспользоваться этой опцией, браузер должен поддерживать криптографическое закрытие (начиная с версии Internet Explorer 3.0 и далее). ООО «Тюмень «Доктор ОСТ» оставляют за собой право предоставлять информацию государственным органам при соответствующих запросах или в случаях, предусмотренных законодательством.

Для удаления информации о Лице из наших контактных списков, необходимо обращаться по следующему адресу: ООО «Тюмень «Доктор ОСТ», г. Тюмень, ул. Мельникайте, д.138а/1.

Лицо может продолжать получать материалы, пока ведется обновление наших списков. Периодически Правила конфиденциальности веб-сайта могут обновляться. После обновления данные правила будут доступны на настоящей странице.

ПРИКАЗ

01.12.2017 г

№ 19

г. Тюмень

Об утверждении Положения о хранении
и использовании персональных данных
в ООО «Тюмень «Доктор ОСТ»

С целью соблюдения положений ст. ст. 23, 26 Конституции РФ, требований ФЗ-152 «О персональных данных», для обеспечения соблюдения законных прав и интересов ООО «Тюмень «Доктор ОСТ», а так же граждан, обращающихся за оказанием услуг, в связи с необходимостью получения, систематизации, хранения и передачи сведений, составляющих персональные данные
п р и к а з ы в а ю:

1. Утвердить Положение о хранении и использовании персональных данных граждан в ООО «Тюмень «Доктор ОСТ» (Приложение № 1).
2. Работникам ООО «Тюмень «Доктор ОСТ» руководствоваться в своей работе и работе медицинского центра утвержденным Положением.
3. Назначить ответственным за хранение и использование персональных данных граждан управляющего медицинским центром ООО «Тюмень «Доктор ОСТ» Толкачеву А.С.
4. Поручить управляющему при приеме сотрудников знакомить работников организации с данным приказом и приложением к нему под расписку.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор



О.В. Кузина

ПОЛОЖЕНИЕ

о хранении и использовании персональных данных

I. Общие положения

1.1. Настоящим Положением определяется порядок обращения с персональными данными граждан и работников в ООО «Тюмень «Доктор ОСТ» (далее - Общество).

1.2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов Общества и граждан, в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные.

1.3. Персональные данные гражданина - любая информация, относящаяся к данному гражданину (субъекту персональных данных) и необходимая Обществу в связи с гражданско-правовыми отношениями, в том числе:

- фамилия, имя, отчество;
- дата и место рождения;
- адрес;
- семейное, социальное, имущественное положение;
- образование, профессия;
- доходы, имущество и имущественные обязательства;
- другая аналогичная информация, на основании которой возможна безошибочная идентификация субъекта персональных данных.

1.4. Сведения о персональных данных относятся к числу конфиденциальных (составляющих охраняемую законом тайну Общества). Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания (см. далее);
- по истечении 75 лет срока их хранения;
- в других случаях, предусмотренных федеральными законами.

1.5. В соответствии с положениями ст. 26 Конституции РФ, Общество принимает на себя обязательства по сохранению конфиденциальности персональных данных, разглашение которых возможно только с согласия гражданина.

II. Основные понятия. Состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

- персональные данные гражданина - в соответствии с определением п. 1.3 настоящего Положения;
- обработка персональных данных гражданина - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;
- конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным сотрудников, требование не допускать их распространения без согласия гражданина или иного законного основания;
- распространение персональных данных - действия, направленные на передачу персональных данных граждан определенному кругу лиц (передача персональных данных) или ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных граждан в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или представление доступа к персональным данным граждан каким-либо иным способом;
- использование персональных данных - действия (операции) с персональными данными, совершаемые уполномоченным должностным лицом Общества в целях принятия решений или

совершения иных действий, порождающих юридические последствия в отношении граждан либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных граждан, в том числе их передачи;

- уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных сотрудников или в результате которых уничтожаются материальные носители персональных данных граждан;

- обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному лицу;

- общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия гражданина, или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

- информация - сведения (сообщения, данные) независимо от формы их представления;

- документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. Информация, представляемая сотрудником при поступлении на работу в Общество, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса РФ лицо, поступающее на работу, предъявляет:

- паспорт или иной документ, удостоверяющий личность;

- трудовую книжку, за исключением случаев, когда договор заключается впервые, или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

- страховое свидетельство государственного пенсионного страхования;

- документы воинского учета - для лиц, подлежащих воинскому учету;

- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

- свидетельство о присвоении ИНН (при его наличии у работника).

2.3. При оформлении сотрудника отделом кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

- сведения о воинском учете;

- данные о приеме на работу;

- сведения об аттестации;

- сведения о повышенной квалификации;

- сведения о профессиональной переподготовке;

- сведения о наградах (поощрениях), почетных званиях;

- сведения об отпусках;

- сведения о социальных гарантиях;

- сведения о месте жительства и о контактных телефонах.

2.4. В отделе кадров Общества создаются и хранятся следующие группы документов, содержащие данные о сотрудниках в единичном или сводном виде:

2.4.1. Документы, содержащие персональные данные:

- комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

- комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность;

- подлинники и копии приказов (распоряжений) по кадрам;

- личные дела и трудовые книжки;

- дела, содержащие основания к приказу по личному составу;

- дела, содержащие материалы аттестаций сотрудников;

- дела, содержащие материалы внутренних расследований;

- справочно-информационный банк данных по персоналу (картотеки, журналы);
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Общества, руководителям структурных подразделений;
- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

2.4.2. Документация по организации работы структурных подразделений:

- положения о структурных подразделениях;
- должностные инструкции работников;
- приказы, распоряжения, указания руководства Общества;
- документы планирования, учета, анализа и отчетности по вопросам кадровой работы.

III. Организация обработки персональных данных граждан

3.1. Обработка персональных данных граждан организуется в соответствии со схемой 1.

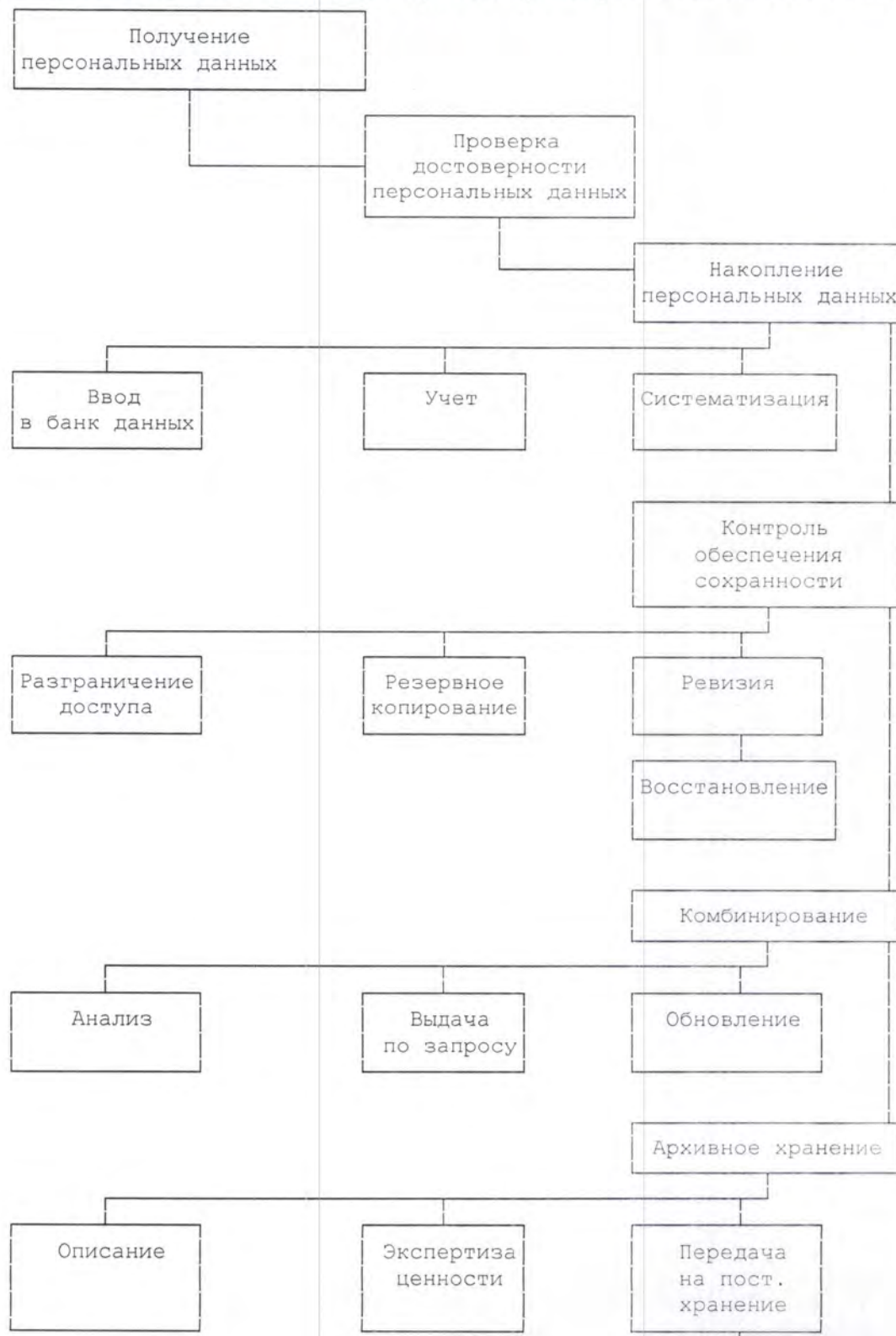


Схема 1

3.2. Все персональные данные гражданина следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то гражданин должен быть уведомлен об этом заранее (в письменной форме) и от него должно быть получено письменное согласие. Должностное лицо предприятия обязано сообщить сотруднику о целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа гражданина дать письменное согласие на их получение.

3.3. Организация не имеет права получать и обрабатывать персональные данные гражданина о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни сотрудника только с его письменного согласия.

3.4. Обработка указанных персональных данных граждан возможна только с их согласия либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья гражданина, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия сотрудника невозможно;
- по требованию полномочных государственных органов - в случаях, предусмотренных федеральным законом.

3.5. Общество вправе обрабатывать персональные данные граждан только с их письменного согласия.

3.6. Письменное согласие гражданина на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (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;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

3.7. Согласие гражданина не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия работодателя;
- обработка персональных данных в целях исполнения трудового договора;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов граждан, если получение его согласия невозможно.

3.8. Сотрудник Общества представляет достоверные сведения о себе.

3.9. В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина руководитель Общества и его законные, полномочные представители при обработке персональных данных сотрудника должны выполнять следующие общие требования:

3.9.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов или иных правовых актов, содействия работникам в трудоустройстве, обучении и профессиональном продвижении, обеспечение личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.9.2. При определении объема и содержания, обрабатываемых персональных данных Общество должно руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

3.9.3. При принятии решений, затрагивающих интересы гражданина, Общество не имеет права основываться на персональных данных, полученных о нем исключительно в результате их автоматизированной обработки или электронного получения.

3.9.4. Защита персональных данных гражданина от неправомерного их использования утраты обеспечивается за счет его средств в порядке, установленном федеральным законом.

3.9.5. Сотрудники и их представители должны быть ознакомлены под расписку с документами Компании, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.9.6. Во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен.

IV. Передача персональных данных

4.1. При передаче персональных данных гражданина работодатель должен соблюдать следующие требования:

4.1.1. Не сообщать персональные данные гражданина третьей стороне без письменного согласия последнего, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом.

4.1.2. Не сообщать персональные данные гражданина в коммерческих целях без его письменного согласия. Обработка персональных данных граждан в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

4.1.3. Предупредить лиц, получивших персональные данные гражданина, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные гражданина, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными сотрудников в порядке, установленном федеральными законами.

4.1.4. Осуществлять передачу персональных данных граждан в пределах Компании в соответствии с настоящим Положением.

4.1.5. Разрешать доступ к персональным данным граждан только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

4.1.6. Не запрашивать информацию о состоянии здоровья гражданина, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции.

4.1.7. Передавать персональные данные гражданина его законным, полномочным представителям в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции.

4.2. Персональные данные сотрудников обрабатываются и хранятся в отделе кадров.

4.3. Персональные данные граждан могут быть получены, проходить дальнейшую обработку и передаваться на хранения, как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

4.4. При получении персональных данных не от гражданина (за исключением случаев, если персональные данные являются общедоступными) Общество до начала обработки таких персональных данных обязано предоставить гражданину следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;

- предполагаемые пользователи персональных данных;
- установленные федеральными законами права субъекта персональных данных.

V. Доступ к персональным данным граждан

5.1. Право доступа к персональным данным граждан имеют:

- руководитель Общества;
- сотрудники отдела кадров;
- сотрудники бухгалтерии;
- начальник отдела экономической безопасности (информация о фактическом месте проживания и контактные телефоны);
- сотрудники секретариата (информация о фактическом месте проживания и контактные телефоны);
- начальник отдела внутреннего контроля (доступ к персональным данным сотрудников в ходе плановых проверок);
- руководители структурных подразделений по направлению деятельности (доступ к персональным данным только граждан своего подразделения).

5.2. Сотрудник Общества имеет право:

5.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копии любой записи, содержащей его персональные данные.

5.2.2. Требовать от работодателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для работодателя персональных данных.

5.2.3. Получать от работодателя:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

5.2.4. Требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия работодателя при обработке и защите его персональных данных.

5.3. Копировать и делать выписки персональных данных сотрудника разрешается исключительно в служебных целях с письменного разрешения начальника отдела кадров.

5.4. Передача информации третьей стороне возможна только при письменном согласии работников.

VI. Ответственность за нарушение норм, регулирующих обработку персональных данных

6.1. Сотрудники Общества, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

6.2. Руководитель Общества за нарушение порядка обращения с персональными данными несет административную ответственность согласно ст. ст. 5.27 и 5.39 Кодекса об административных правонарушениях РФ, а также возмещает сотруднику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные об этом сотруднике.

ПРИКАЗ

01.12.2017 г

№ 22

г. Тюмень

Об утверждении Положения об ответственном лице,
осуществляющем функции по организации защиты
персональных данных в ООО «Тюмень «Доктор ОСТ»

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», во исполнение постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

п р и к а з ы в а ю:

1. Назначить управляющего медицинским центром ООО «Тюмень «Доктор ОСТ» Толкачеву Анастасию Юрьевну ответственным за обеспечение защиты персональных данных пациентов, работников и контрагентов в ООО «Тюмень «Доктор ОСТ».

2. Утвердить положение об ответственном лице, осуществляющем функции по организации защиты персональных данных в ООО «Тюмень «Доктор ОСТ» (Приложение №1).

3. Руководителям структурных подразделений главного врача, управляющего, как работников, осуществляющих сбор персональных данных, ознакомить с настоящим приказом под роспись работников.

4. Контроль за исполнением настоящего приказа оставляю за собой.

5. Приказ вступает в силу со дня его подписания.

Директор



О.В. Кузина

ПОЛОЖЕНИЕ ОБ ОТВЕТСТВЕННОМ ЛИЦЕ, ОСУЩЕСТВЛЯЮЩЕМ ФУНКЦИИ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Положение об ответственном лице, осуществляющем функции по организации защиты персональных данных (далее – ПДн), обеспечению безопасности ПДн при их обработке в информационных системах персональных данных в ООО «Тюмень «Доктор ОСТ» (далее – Положение) разработано на основании требований нормативно-методических документов Российской Федерации в области защиты персональных данных.

2. Настоящее Положение устанавливает требования к полномочиям и обязанностям ответственного за обеспечение защиты ПДн должностного лица (далее – ответственное лицо) Толкачеву А.Ю. при их обработке в информационных системах персональных данных (далее ИСПДн) в ООО «Тюмень «Доктор ОСТ». При этом, обрабатываемые ПДн представляют собой совокупность ПДн, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации (далее информационные системы) или без использования таковых.

3. Под техническими средствами, позволяющими осуществлять обработку ПДн, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

4. Ответственное лицо назначается приказом директора и обеспечивает безопасность ПДн путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

5. Ответственное лицо обеспечивает безопасность ПДн при их обработке в информационных системах с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

6. Для обеспечения безопасности ПДн, при их обработке в информационных системах, ответственное лицо обеспечивает защиту речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

7. Методы и способы защиты информации в ИСПДн устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

8. Ответственное лицо обеспечивает достаточность принятых мер по организации безопасной обработки ПДн в информационных системах, оцениваемой при проведении государственного контроля и надзора.

Работы по обеспечению безопасности ПДн при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

9. Ответственное лицо обеспечивает применение средств защиты информации в информационных системах, прошедших в установленном порядке процедуру оценки соответствия.

10. Ответственное лицо обеспечивает и организует разработку организационной, технической документации на ИСПДн и подготовку информационной системы к проведению оценки соответствия (аттестации).

11. При проведении классификации ИСПДн ответственное лицо руководствуется порядком проведения классификации ИСПДн устанавливаемым совместно Федеральной службой по техническому и экспортному контролю Российской Федерации.

12. Ответственное лицо обеспечивает обмен персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

13. Ответственное лицо обеспечивает размещение информационных систем, специального оборудования и охрану помещений, в которых ведется работа с ПДн, организацию режима безопасности в этих помещениях при котором обеспечивается сохранность носителей ПДн и средств защиты информации, а также исключается возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

14. Возможные каналы утечки информации при обработке ПДн в информационных системах определяются Федеральной службой по техническому и экспортному контролю Российской Федерации и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

15. Пользователями ИСПДн являются сотрудники, обрабатывающие ПДн в информационной системе, отвечающие за обеспечение конфиденциальности ПДн и безопасности ПДн в информационной системе на своем рабочем месте.

16. При обработке ПДн в информационной системе

- ответственное лицо обеспечивает и требует от пользователей ИСПДн в рамках их компетенции:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к ПДн;

в) недопущение воздействия на технические средства автоматизированной обработки ПДн в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности ПДн.

17. Мероприятия по обеспечению безопасности ПДн при их обработке в информационных системах организуются и проводятся ответственным лицом и включают в себя:

а) определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПД, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение Пользователей ИСПДн, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

ж) учет Пользователей ИСПДн, допущенных к работе с ПДн в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты ПДн.

18. Сотрудники, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании списка, утвержденного ответственным лицом и согласованного с администратором информационной безопасности ИСПДн.

19. Ответственное лицо обеспечивает регистрацию запросов Пользователей информационной системы на получение ПДн, а также факты предоставления ПДн по этим запросам в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется ответственным лицом и администратором информационной безопасности ИСПДн.

20. При обнаружении нарушений порядка предоставления ПДн администратор информационной безопасности ИСПДн по распоряжению ответственного лица незамедлительно приостанавливает предоставление ПДн пользователям информационной системы до выявления причин нарушений и устранения этих причин.