Приложение 2

Утверждено

Приказом генерального директора

от «10» февраля 2020г № 10-0

Положение

об обработке персональных данных клиентов в ООО «Таврия»

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским Кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными документами в сфере обработки персональных данных.

1.2. Целью данного Положения является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, от несанкционированного доступа, неправомерного их использования или утраты, в том числе защиты прав на неприкосновенность частной жизни, личную, семейную и врачебную тайну.

1.3. Положение определяет порядок и условия обработки персональных данных клиентов Общества с ограниченной ответственностью «Таврия» (далее - Санаторий) с использованием средств автоматизации и без использования таких средств.

1.4. Обработка персональных данных осуществляется в целях, непосредственно связанных с деятельностью Санатория:

- оказание санаторно-курортной медицинской помощи;
- оказание платных медицинских услуг;
- оказание иных платных услуг, не связанных с лечением: транспортные услуги, услуги средств размещения, услуги питания, услуги в сфере сервисного и бытового обслуживания клиентов, услуги по организации физкультурно-оздоровительных, спортивных и культурно-развлекательных мероприятий, экскурсионные услуги.

Санаторий собирает персональные данные только в объеме, необходимом для достижения названных целей.

1.5. В настоящем Положении используются следующие понятия, термины и сокращения:

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, профессия, другая информация, необходимая ООО «Таврия» Персональные данные граждан являются конфиденциальной, строго охраняемой в силу закона информацией.

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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

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

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

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

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.

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

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

Субъект персональных данных (клиент) - физическое лицо, получившее/приобретшее путевки на санаторно-курортное лечение в Санаторий, медицинские и иные услуги, не связанные с лечением.

2. Состав персональных данных клиентов

2.1. К персональным данным клиентов, которые обрабатывает Санаторий, относятся:

- анкетные и биографические данные (ФИО субъекта персональных данных, дата и место рождения);
- сведения о составе семьи;
- информация о детях (ФИО и дата рождения ребенка);
- данные документа, удостоверяющего личность;
- адрес места жительства (места регистрации);
- контактный телефон, электронная почта;

- место работы, должность, образование, трудовой статус;
- № комнаты, предоставленной для проживания, срок пребывания в Санатории;
- сведения о приобретенной путевке (стоимость, продолжительность, реквизиты);
- данные анамнеза, медицинского обследования (клинического, лабораторного, инструментального);
- диагноз заболевания;
- другая аналогичная информация, на основании которой возможна безошибочная идентификация субъекта персональных данных

2.2. К документам, содержащим персональные данные клиентов относятся:

- анкеты;
- история болезни;
- санаторно-курортная карта;
- санаторно-курортная книжка;
- добровольное информационное согласие на медицинское вмешательство;
- санаторно-курортная путевка;
- обменные путевки, ваучеры, направления на лечение и отдых;
- заявки на бронирование номеров;
- списки отдыхающих, направляемых на экскурсии;
- медицинские журналы, связанные с отпуском лечебных процедур;
- договоры на приобретение санаторно-курортных услуг, иные договоры.

Указанные документы относятся к конфиденциальной информации ограниченного доступа.

3. Основные принципы обработки персональных данных

3.1. Обработка персональных данных клиентов осуществляется на основе следующих принципов:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;
- обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- обрабатываемые персональные данные клиентов подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

- личная ответственность сотрудников Санатория за сохранность и конфиденциальность персональных данных клиентов, а также носителей этой информации;
- наличие четкой разрешительной системы доступа сотрудников Санатория к документам и базам данных, содержащим персональные данные.

3.2. При обработке персональных данных клиентов обеспечивается их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

3.3. Хранение персональных данных клиентов осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, является субъект персональных данных.

4. Требования к обработке персональных данных

4.1. В целях обеспечения прав и свобод человека и гражданина работники Санатория при обработке персональных данных клиентов, обязаны соблюдать следующие общие требования:

- обработка персональных данных осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения личной безопасности, контроля количества и качества оказываемых услуг;
- при определении объема и содержания, обрабатываемых персональных данных работники Санатория должны руководствоваться Конституцией Российской Федерации, иными федеральными законами;
- обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также сведений о членстве субъекта персональных данных в общественных объединениях не допускается;
- обработка персональных данных клиентов осуществляется только специально уполномоченными лицами, которым это необходимо для выполнения непосредственных должностных обязанностей;
- использование персональных данных возможно только в соответствии с целями, определившими их получение;
- персональные данные клиентов не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации;
- при принятии решений, затрагивающих интересы клиента, работники Санатория не имеют права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки.

5. Получение персональных данных

5.1. Все персональные данные следует получать непосредственно от клиента. Клиент самостоятельно принимает решение о предоставление своих персональных данных и дает письменное согласие на их обработку.

Отказ клиента в предоставление своих персональных данных дает Санаторию право отказать клиенту в оказании услуги в случае если персональные данные являются для этого необходимыми.

5.2. Письменное согласие клиента на обработку его персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта, 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 работника;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению, 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, а также способ его отзыва.

5.3. Согласие на обработку персональных данных может быть отозвано клиентом.

5.4. Сведения, которые характеризуют физиологические и биологические особенности клиента и на основе которых можно установить его личность (биометрические персональные данные), и которые используются для установления личности клиента, могут обрабатываться Санаторием только при наличии согласия клиента в письменной форме.

5.5. Санаторий осуществляет сбор персональных данных, в том числе с использованием информационно-телекоммуникационной сети Интернет через официальный https://tavria-crimea.com/ в случаях:

- онлайн-бронирования номера и заказа санаторно-курортных путевок;

- обращения клиента путем использования сервиса «Заказать звонок» или «Задать вопрос»

В данном случае Санаторий обеспечивает возможность доступа клиентов к документу, определяющему политику в отношении обработки персональных данных, и сведениях о реализуемых требованиях к защите персональных данных.

Для этих целей в открывающихся окнах вкладок «Заказать звонок», «Задать вопрос» «Бронирование номеров» на официальном сайте https://tavria-crimea.com/ субъект персональных данных (клиент) имеет возможность использовать соответствующую гиперссылку, указывающую на страницу сайта, на котором размещены вышеуказанные документы.

При этом в открывающихся окнах вкладок «Заказать звонок», «Задать вопрос», «Бронирование номеров» при заказе звонка, направлении вопроса, бронировании номера после введения клиентом всех своих данных предусмотрено появление всплывающего окна, содержание которого предусматривает обязательное подтверждение клиентом в ознакомлении с политикой в отношении обработки персональных данных ознакомлен и согласии на обработку своих персональных данных, передаваемых Санаторию при заказе звонка, направлении вопроса или бронировании номера через информационно-телекоммуникационную сеть Интернет.

Электронное подтверждение клиента о согласии на обработку персональных данных является тождественным согласию, полученным в письменном виде.

6. Обеспечение конфиденциальности персональных данных

6.1. Персональные данные относятся к категории конфиденциальной информации.

6.2. Работниками Санатория, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

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

6.4. Хранение персональных данных клиентов может осуществляться на бумажных и электронных носителях, доступ к которым ограничен списком лиц, допущенных к обработке персональных данных.

6.5. Все электронные носители персональных данных подлежат строгому учету.

6.6. Хранение персональных данных клиентов должно происходить в порядке, исключающем их утрату или их неправомерное использование.

6.7. Персональные данные клиентов, содержащиеся на бумажных носителях и отчуждаемых электронных носителях информации, должны храниться в сейфах или запираемых шкафах, установленных в пределах контролируемой зоны.

6.8. Персональные данные клиентов, содержащиеся на электронных носителях информации, должны храниться на автоматизированных рабочих местах и серверах информационных систем, установленных в пределах контролируемой зоны.

6.9. Все меры, направленные на соблюдение конфиденциальности при сборе, обработке и хранении персональных данных субъекта, распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

7. Передача персональных данных

7.1. При передаче персональных данных клиентов должны соблюдаться следующие требования:

- персональные данные не могут быть переданы третьей стороне без письменного согласия клиента или его законного представителя, за исключением случаев, когда

это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных федеральными законами;

- лица, получающие персональные данные клиентов, должны предупреждаться о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц обеспечения конфиденциальности полученных персональных данных;
- персональные данные клиентов не могут передаваться для использования в коммерческих целях без его письменного согласия клиента;
- персональные данные клиентов не должны передаваться по телефону или факсу.

8. Уничтожение персональных данных

8.1. Обрабатываемые персональные данные должны быть уничтожены в следующих случаях:

- в случае достижения цели обработки персональных данных - в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных - в срок, не превышающий тридцати дней с даты поступления указанного отзыва;
- в случае выявления неправомерной обработки с персональными данными и невозможности устранения допущенных нарушений - в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных.

8.2. После уничтожения персональных данных необходимо уведомить об этом субъекта персональных данных или его законного представителя.

8.3. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

8.4. В случае отсутствия возможности уничтожения персональных данных в течение, указанных выше сроков, Санаторий осуществляет блокирование таких персональных данных и обеспечивает их уничтожение в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

9. Права и обязанности сторон при обработке персональных данных

9.1. В целях обеспечения прав и свобод человека и гражданина Санаторий при обработке персональных данных Клиента обязан соблюдать следующие общие требования:

- обработка персональных данных клиента может осуществляться исключительно в целях оказания законных услуг клиентам;
- персональные данные клиента следует получать у него самого. Если персональные данные клиента возможно получить только у третьей стороны, то клиент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие;
- сотрудники Санатория должны сообщить клиентам о целях, предполагаемых источниках и способах получения персональных данных, а также о характере

подлежащих получению персональных данных и последствиях отказа клиента дать письменное согласие на их получение;

- при наличии надлежащим образом оформленного запроса предоставлять клиенту доступ к его персональным данным;
- хранение и защита персональных данных клиента от неправомерного их использования или утраты должна быть обеспечена Санаторием за счет его средств в порядке, установленном законодательством;
- в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу клиента либо уполномоченного органа по защите прав субъектов персональных данных Санаторий обязан осуществить блокирование персональных данных на период проверки;
- в случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных клиентом либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование;
- в случае отзыва клиентом согласия на обработку своих персональных данных Санаторий обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней, если иное не предусмотрено соглашением между Санаторием и Клиентом.

9.2. Каждый субъект персональных данных имеет право:

- на получение полной информации о своих персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных действующим законодательством;
- на определение форм и способов обработки персональных данных;
- на отзыв согласия на обработку персональных данных;
- ограничивать способы и формы обработки персональных данных, запрет на распространение персональных данных без его согласия;
- обжаловать неправомерные действия или бездействия по обработке персональных данных и требовать соответствующей компенсации в суде;
- на дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения;
- определять представителей для защиты своих персональных данных;
- требовать уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные клиента, обо всех произведенных в них изменениях или исключениях из них;
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

10. Защита персональных данных

10.1. Санаторий при обработке персональных данных обязано принимать необходимые организационные и технические меры для защиты персональных данных клиентов от

неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

10.2. Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, используемых в процессе деятельности Санатория.

10.3. Основными организационными мерами по защите персональных данных являются:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое, избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- обеспечение знания сотрудником требований нормативно-методических документов по защите информации и сохранении тайны;
- обеспечение наличия необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- грамотная организация процесса уничтожения информации;
- организация регулярной воспитательной и разъяснительной работы с сотрудниками по предупреждению утраты и утечки сведений при работе с конфиденциальными документами, содержащими персональные данные;
- разработка комплекта внутренних документов, регламентирующих процессы обработки персональных данных.

10.4. В качестве дополнительных организационных мер защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ к персональным данным с целью овладения ценными сведениями и их использования, а также их искажения, уничтожения, подмены, фальсификации содержания реквизитов документа и т.д.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Санатория. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов, содержащих персональные данные.

10.5. В качестве технических мер защиты персональных данных применяются антивирусная защита, межсетевые экраны, разграничение прав доступа (пароли), специализированные средства защиты информации от несанкционированного доступа.

11. Ответственность за разглашение персональных данных и нарушение

11.1. Санаторий несет ответственность за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность сотрудников за соблюдением, установленных в организации принципов уважения приватности.

11.2. Каждый работник, получающий доступ к конфиденциальному документу, содержащему персональные данные клиента, несет личную ответственность за сохранность носителя и конфиденциальность информации.

11.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами и полную материальную ответственность в случае причинения их действиями ущерба в соответствии с Трудовым кодексом Российской Федерации.

11.4. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также требований к защите персональных данных, установленных в соответствии с Законом, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

11.5. Санаторий обязуется поддерживать систему приема, регистрации и контроля рассмотрения жалоб клиентов, доступную как посредством использования Интернета, так и с помощью телефонной, телеграфной или почтовой связи.

11.3. Жалобы и заявления по поводу соблюдения требований обработки персональных данных рассматриваются в десятидневный срок со дня поступления. Сотрудники Санатория обязаны на должном уровне обеспечивать рассмотрение запросов, заявлений и жалоб клиентов, а также содействовать исполнению требований компетентных органов.

12. Заключительные положения

12.1. Настоящее Положение и изменения к нему утверждаются генеральным директором ООО «Таврия» и вводятся в действие его приказом.

12.2. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно, до замены его новым Положением.

12.3. Настоящее Положение является обязательным для исполнения всеми сотрудниками ООО «Таврия» непосредственно осуществляющими обработку персональных данных и (или) имеющими доступ к персональным данным.