

к приказу АО «Курорт Старая Русса»

от «7» сентября 2023 г. № 142

ПОЛОЖЕНИЕ

«О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ

АО «Курорт Старая Русса»

г. Старая Русса

«07» сентября 2023 г.

1. Общие положения

1.1. Настоящее Положение регламентируется Конституцией Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации» N 149-ФЗ от 27.07.2006 года, Федеральным законом «О персональных данных» N 152-ФЗ от 27.07.2006 года и другими нормативно правовыми актами.

1.2. Основные понятия, используемые в Положении:

- Санаторий - организация, предоставляющая санаторно-курортные и гостиничные услуги клиенту;
- клиент - физическое лицо, потребитель санаторно-курортных и гостиничных услуг, субъект персональных данных;
- санаторно-курортные услуги — действия Санатория по санаторно-курортному обслуживанию (проживание питание, лечение), а также иная деятельность которая включает в себя основные и дополнительные медицинские услуги, предоставляемые Клиенту;
- гостиничные услуги - действия Санатория по размещению Клиентов в объекте размещения, а также иная деятельность, связанная с размещением и проживанием, которая включает в себя основные и дополнительные услуги, предоставляемые Клиенту;
- персональные данные - информация, сохраненная в любом формате, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), которая сама по себе или в сочетании с другой информацией, имеющейся в распоряжении Санатория, позволяет идентифицировать личность Клиента;
- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

1.3. Настоящим Положением устанавливается порядок обработки персональных данных Клиентов, для которых Санаторием осуществляется весь спектр услуг по санаторно-курортному лечению, приему и размещению в санатории.

1.4. Целью Положения является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

1.5. Персональные данные обрабатываются в целях исполнения договора по предоставлению санаторно-курортных услуг, медицинских услуг, услуг по проживанию или временному размещению, одной из сторон которого является Клиент. Санаторий собирает данные только в объеме, необходимом для достижения названной цели.

1.6. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

1.7. Настоящее Положение утверждается директором и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным Клиента.

2. Состав и получение персональных данных Клиентов

2.1. К персональным данным, сбор и обработку которых осуществляет Санаторий, относятся:

- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения, место рождения.);
- паспортные данные (серия и номер паспорт, орган и дата выдачи);
- адрес регистрации;
- адрес места жительства;
- номер контактного телефона;
- адрес электронной почты;
- медицинские (данные о диагнозе, лабораторных и функциональных исследованиях, динамике состояния, назначенном лечении и его результате).

2.2. Все персональные данные сотрудники Санатория получают непосредственно от субъекта персональных данных - Клиентов.

3. Обработка и хранение персональных данных Клиентов

3.1. Обработка персональных данных Санатория в интересах Клиентов заключается в получении, систематизации, накоплении, хранении, уточнении (обновлении, изменении), использовании, распространении, обезличивании, блокировании, уничтожении и в защите от несанкционированного доступа персональных данных Клиентов.

3.2. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

3.3. Обработка персональных данных Клиентов ведется методом смешанной обработки.

3.4. К обработке персональных данных Клиентов могут иметь доступ только сотрудники Санатория, допущенные к работе с персональными данными Клиента и подписавшие Соглашение о неразглашении персональных данных Клиента.

3.5. Перечень сотрудников Санатория, имеющих доступ к персональным данным Клиентов, определяется приказом генерального директора.

3.6. Персональные данные Клиентов на бумажных носителях хранятся в архиве Санатория. До сдачи в архив персональные данные, за исключением медицинских, хранятся в сейфе в кабинете старшего администратора, медицинские - в кабинете сбора медицинской документации.

3.7. Персональные данные Клиентов в электронном виде хранятся в локальной компьютерной сети Санатория, в электронных папках и файлах в персональных компьютерах руководителя службы внутреннего контроля и сотрудников, допущенных к обработке персональных данных Клиентов.

4. Использование и передача персональных данных Клиентов

4.1. Использование персональных данных Клиентов осуществляется Санаторием исключительно для достижения целей, определенных договором между Клиентом и Санаторием, в частности, для предоставления санаторно-курортных услуг, медицинских услуг, услуг по проживанию или временному размещению, а также дополнительных услуг.

4.2. При передаче персональных данных Клиентов Санаторий должен соблюдать следующие требования:

4.2.1. Предупредить лиц, получающих персональные данные Клиентов 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 Клиентов, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется в случае обезличивания персональных данных и в отношении общедоступных данных.

4.2.2. Разрешать доступ к персональным данным Клиентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

4.2.3. При трансграничной передаче персональных данных Санаторий обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

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

- наличия согласия в письменной форме Клиента;
- предусмотренных международными договорами Российской Федерации по вопросам выдачи виз, международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам, а также международными договорами Российской Федерации о реадмиссии;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

4.3. Не допускается отвечать на вопросы, связанные с передачей информации, содержащей персональные данные, по телефону или факсу.

4.4. Санаторий вправе предоставлять или передавать персональные данные Клиентов третьим лицам в следующих случаях:

- если раскрытие этой информации требуется для соблюдения закона, выполнения судебного акта;
- для оказания содействия в проведении расследований, осуществляемых правоохранительными или иными государственными органами;
- для защиты законных прав Клиента и Санатория.

5. Защита персональных данных Клиентов от несанкционированного доступа

5.1. Санаторий обязан при обработке персональных данных Клиентов принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

5.2. Для эффективной защиты персональных данных Клиентов необходимо:

5.2.1. соблюдать порядок получения, учета и хранения персональных данных Клиентов;

5.2.2. применять технические средства охраны, сигнализации;

5.2.3. заключить со всеми сотрудниками, связанными с получением, обработкой и защитой персональных данных Клиента, Соглашение о неразглашении персональных данных Клиента;

5.2.4. привлекать к дисциплинарной ответственности сотрудников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных Клиента.

5.3. Допуск к персональным данным Клиентов сотрудников Санатория, не имеющих надлежащим образом оформленного доступа, запрещается.

5.4. Документы, содержащие персональные данные Клиентов, хранятся в кабинете сотрудников Ресепшн, обеспечивающем защиту от несанкционированного доступа.

5.5. Защита доступа к электронным базам данных, содержащим персональные данные Клиентов, обеспечивается принятием организационных и технических мер защиты информации, обеспечивающих необходимый уровень защищенности в соответствии с действующим законодательством.

5.6. Копировать и делать выписки персональных данных Клиента разрешается исключительно в служебных целях с письменного разрешения руководителя.

6. Обязанности Санатория

6.1. Санаторий обязан:

6.1.1. Осуществлять обработку персональных данных Клиентов исключительно в целях оказания законных услуг Клиентам.

6.1.2. Получать персональные данные Клиента непосредственно 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.

6.1.3. Не получать и не обрабатывать персональные данные Клиента о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных законом.

6.1.4. Предоставлять доступ к своим персональным данным Клиенту или его законному представителю при обращении либо при получении запроса, содержащего номер основного документа, удостоверяющего личность Клиента или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись Клиента или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации. Сведения о наличии персональных данных должны быть предоставлены Клиенту в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

6.1.5. Ограничивать право Клиента на доступ к своим персональным данным, если:

- 1) обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- 2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- 3) предоставление персональных данных нарушает конституционные права и свободы других лиц.

6.1.6. Обеспечить хранение и защиту персональных данных Клиента от неправомерного их использования или утраты.

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

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

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

7. Права Клиента

7.1. Клиент имеет право на:

- доступ к информации о самом себе, в том числе содержащей информацию подтверждения факта обработки персональных данных, а также цель такой обработки; способы обработки персональных данных, применяемые Санаторием; 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 Клиента может повлечь за собой обработка его персональных данных;
- определение форм и способов обработки его персональных данных;
- ограничение способов и форм обработки персональных данных;
- запрет на распространение персональных данных без его согласия;
- изменение, уточнение, уничтожение информации о самом себе;
- обжалование неправомерных действий или бездействий по обработке персональных данных и соответствующую компенсацию в судебном порядке.

8. Использование персональных данных Клиентов для рекламы и маркетинговых исследований

8.1. Субъект персональных данных предоставляет Санаторию согласие на осуществление рекламно-информационной рассылки о скидках, акциях, новых предложениях и т. д., с помощью различных средств связи. Включая но не ограничиваясь: почтовая рассылка, электронная почта, телефон, сеть Интернет, социальные сети и т. д. Периодичность таких рассылок определяется Санаторием на его усмотрение в одностороннем порядке.

Клиент вправе отказаться от получения рекламной и другой информации без объяснения причин отказа. При этом, если Клиент не желает получать указанные рассылки он должен сообщить об этом по телефону содержащемуся в письме с рассылкой или путем отправки сообщения по электронной почте, указанной на сайте.

9. Конфиденциальность персональных данных Клиентов

9.1. Сведения о персональных данных Клиентов, являются конфиденциальными.

9.2. Санаторий обеспечивает конфиденциальность персональных данных и обязана не допускать их распространения третьим лицам без согласия Клиентов либо наличия иного законного основания.

9.3. Лица, имеющие доступ к персональным данным Клиентов, обязаны соблюдать режим конфиденциальности, они должны быть предупреждены о необходимости соблюдения режима секретности. В связи с режимом конфиденциальности информации персонального характера должны предусматриваться соответствующие меры безопасности для защиты данных от случайного или несанкционированного уничтожения, от случайной утраты, от несанкционированного доступа к ним, изменения или распространения.

9.4. Все меры конфиденциальности при сборе, обработке и хранении персональных данных Клиентов распространяются на все носители информации как на бумажные, так и на автоматизированные.

9.5. Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

10. Ответственность за нарушение норм, регулирующих обработку персональных данных Клиентов

10.1. Санаторий несет ответственность за персональную информацию, которая находится в ее распоряжении и закрепляет персональную ответственность сотрудников за соблюдением установленного режима конфиденциальности.

10.2. Каждый сотрудник, получающий для работы документ, содержащий персональные данные Клиента, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

10.3. Любое лицо может обратиться к сотруднику Санатория с жалобой на нарушение данного Положения. Жалобы и заявления по поводу соблюдения требований обработки данных рассматриваются в трехдневный срок со дня поступления.

10.4. Сотрудники Санатория обязаны на должном уровне обеспечивать рассмотрение запросов, заявлений и жалоб Клиентов, а также содействовать исполнению требований компетентных органов.

10.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Клиентов, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Генеральный директор
АО «Курорт Старая Русса»



А.В. Репникова