

## ПОЛОЖЕНИЕ

### Об обработке и защите персональных данных обрабатываемых в АО «Санаторий «Родник»

#### 1. Общие положения

1.1. Настоящее Положение является локальным нормативным актом АО «Санаторий «Родник» (далее - Общество), принятым с учетом требований, в частности, гл. 14 Трудового кодекса РФ, Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных).

1.2. В Положении устанавливаются:

- цель, порядок и условия обработки персональных данных;
- категории субъектов, персональные данные которых обрабатываются, категории (перечни) обрабатываемых персональных данных, способы, сроки их обработки и хранения, порядок уничтожения таких данных при достижении целей обработки или при наступлении иных законных оснований;
- положения, касающиеся защиты персональных данных, процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в области персональных данных, на устранение последствий таких нарушений.

1.3. В Положении используются термины и определения в соответствии с их значениями, определенными в Законе о персональных данных.

1.4. Положение вступает в силу с момента его утверждения генеральным директором и действует до его отмены приказом генерального директора или до введения нового Положения.

1.5. Внесение изменений в Положение производится приказом генерального директора. Изменения вступают в силу с момента подписания соответствующего приказа.

#### 2. Категории субъектов персональных данных

2.1. К субъектам, персональные данные которых обрабатываются в Обществе в соответствии с Положением, относятся:

- 1) работники;
- 2) соискатели;
- 3) родственники работников;
- 4) уволенные работники;
- 5) студенты;
- 6) клиенты;
- 7) посетители сайта;
- 8) законные представители;
- 9) контрагенты
- 10) представители контрагентов

#### 3. Цели обработки персональных данных, категории (перечни) обрабатываемых персональных данных

##### 3.1. Цель 1.

3.1.1. Согласно Положению, персональные данные обрабатываются с целью применения и исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ними отношений, в том числе:

- при содействии в трудоустройстве;
- ведении кадрового и бухгалтерского учета;
- содействии работникам в получении образования и продвижении по службе;

- оформлении наградений и поощрений;
- предоставлении со стороны Общества установленных законодательством условий труда, гарантий и компенсаций;
- заполнении и передаче в уполномоченные органы требуемых форм отчетности;
- обеспечении личной безопасности работников и сохранности имущества;
- осуществлении контроля за количеством и качеством выполняемой работы.

3.1.2. В соответствии с целью, указанной в п. 3.1.1. Положения, в Обществе обрабатываются следующие персональные данные:

- фамилия,
- имя,
- отчество;
- год рождения;
- место рождения;
- дата рождения;
- месяц рождения;
- семейное положение;
- социальное положение;
- доходы;
- пол;
- адрес электронной почты;
- адрес место жительства;
- адрес регистрации;
- номер телефона;
- СНИЛС;
- ИНН;
- гражданство;
- данные документа, удостоверяющего личность;
- данные водительского удостоверения;
- данные документа, удостоверяющего личность за пределами Российской Федерации;
- данные документа, содержащиеся в свидетельстве о рождении;
- реквизиты банковской карты;
- номер лицевого счета;
- профессия;
- должность;
- сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- отношение к воинской обязанности;
- сведения о воинском учете;
- сведения об образовании;
- сведения о состоянии здоровья;
- сведения о судимости.

3.1.3. Общество не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

## 3.2. Цель 2.

3.2.1. Согласно Положению, персональные данные обрабатываются с целью оказания клиентам санаторно-курортных, оздоровительных, медицинских, гостиничных и дополнительных услуг.

3.2.2. В соответствии с целью, указанной в п. 3.2.1. Положения, в Обществе обрабатываются следующие персональные данные:

- фамилия,
- имя,
- отчество;
- год рождения;

- место рождения;
- дата рождения;
- месяц рождения;
- семейное положение;
- пол;
- адрес электронной почты;
- адрес место жительства;
- адрес регистрации;
- номер телефона;
- СНИЛС;
- гражданство;
- данные документа, удостоверяющего личность;
- данные документа, удостоверяющего личность за пределами Российской Федерации;
- данные документа, содержащиеся в свидетельстве о рождении;
- реквизиты банковской карты;
- номер лицевого счета.

3.2.3. из специальных категорий персональных данных, Общество осуществляет обработку касающихся состояния здоровья.

### 3.3. Цель 3.

3.3.1. Согласно Положению, персональные данные обрабатываются с целью подготовки, заключению и исполнению гражданско-правового договора.

3.3.2. В соответствии с целью, указанной в п. 3.3.1. Положения, в Обществе обрабатываются следующие персональные данные:

фамилия,

- имя,
- отчество;
- год рождения;
- место рождения;
- дата рождения;
- месяц рождения;
- пол;
- адрес электронной почты;
- адрес место жительства;
- адрес регистрации;
- номер телефона;
- гражданство;
- данные документа, удостоверяющего личность;
- реквизиты банковской карты;
- номер расчетного счета;
- номер лицевого счета.

3.3.3. Общество не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

## 4. Порядок и условия обработки персональных данных

4.1. До начала обработки персональных данных Общество обязано уведомить Роскомнадзор о намерении осуществлять обработку персональных данных.

4.2. Правовым основанием обработки персональных данных для цели, указанной в п. 3.1.1. Положения являются согласие субъекта персональных данных на обработку его персональных данных, Устав АО «Санаторий «Родник», Гражданский кодекс РФ, Трудовой кодекс РФ, Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных", положение об обработке персональных данных в АО «Санаторий «Родник», трудовые договоры, гражданско-правовые договоры, анкеты соискателей.

4.3. Правовым основанием обработки персональных данных для цели, указанной в п. 3.2.1. Положения являются согласие субъекта персональных данных на обработку его персональных данных, Устав АО «Санаторий «Родник», Гражданский кодекса РФ, Федеральный закон от 27.07.2006 N 152-ФЗ "О

персональных данных", Постановление Правительства РФ от 18.11.2020 г. №1853 «Об утверждении Правил предоставления гостиничных услуг в РФ», Постановление Правительства РФ от 17 июля 1995г. №713 «Об утверждении Правил регистрации и снятия граждан РФ с регистрационного учета по месту пребывания и месту жительства в пределах РФ и перечня лиц, ответственных за прием и передачу в органы регистрационного учета документов для регистрации и снятия с регистрационного учета граждан РФ по месту пребывания и по месту жительства в пределах РФ», договор с субъектами персональных данных, анкеты гостя, положение об обработке персональных данных в АО «Санаторий «Родник», лицензия на медицинскую деятельность № Л041-01126-23/00327684 от 14.09.2018 г.

4.4. Правовым основанием обработки персональных данных для цели, указанной в п. 3.3.1. Положения являются согласие субъекта персональных данных на обработку его персональных данных, Устав АО «Санаторий «Родник», Гражданский кодекс РФ, Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных", договор на оказание услуг.

4.5. Обработка персональных данных осуществляется с соблюдением принципов и условий, предусмотренных законодательством в области персональных данных и настоящим Положением.

4.6. Обработка персональных данных в Обществе выполняется следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

4.7. Обработка персональных данных в Обществе осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством в области персональных данных.

4.8. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 Закона о персональных данных.

Согласие на обработку таких персональных данных оформляется отдельно от других согласий на обработку персональных данных. Согласие предоставляется субъектом персональных данных лично либо в форме электронного документа, подписанного электронной подписью, с использованием информационной системы Роскомнадзора.

4.9. Обработка биометрических персональных данных допускается только при наличии письменного согласия субъекта персональных данных. Исключения составляют ситуации, предусмотренные ч. 2 ст. 11 Закона о персональных данных.

4.10. Общество не осуществляет трансграничную передачу персональных данных.

4.7. Обработка персональных данных осуществляется путем сбора, систематизации, хранения, уточнения (обновления, изменения), использования, передачи (предоставления, доступа), обезличивания, удаления, уничтожения персональных данных, в том числе с помощью средств вычислительной техники.

4.7.1. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных в Обществе осуществляются посредством:

- получения оригиналов документов либо их копий;
- копирования оригиналов документов;
- внесения сведений в учетные формы на бумажных и электронных носителях;
- создания документов, содержащих персональные данные, на бумажных и электронных носителях;
- внесения персональных данных в информационные системы персональных данных.

4.7.2. В Обществе используются следующие информационные системы:

- корпоративная электронная почта;
- система электронного документооборота;
- система поддержки рабочего места пользователя;
- система нормативно-справочной информации;
- система управления персоналом;
- система контроля за удаленным доступом;
- информационный портал.

4.8. Передача (распространение, предоставление, доступ) персональных данных субъектов персональных данных осуществляется в случаях и в порядке, предусмотренных законодательством в области персональных данных и Положением.

## 5. Сроки обработки и хранения персональных данных

5.1. Обработка персональных данных в Обществе прекращается в следующих случаях:

- при выявлении факта неправомерной обработки персональных данных. Срок прекращения обработки - в течение трех рабочих дней с даты выявления такого факта;
- при достижении целей их обработки (за некоторыми исключениями);
- по истечении срока действия или при отзыве субъектом персональных данных согласия на обработку его персональных данных (за некоторыми исключениями), если в соответствии с Законом о персональных данных их обработка допускается только с согласия;
- при обращении субъекта персональных данных к Обществу с требованием о прекращении обработки персональных данных (за исключением случаев, предусмотренных ч. 5.1 ст. 21 Закона о персональных данных). Срок прекращения обработки - не более 10 рабочих дней с даты получения требования (с возможностью продления не более чем на пять рабочих дней, если направлено уведомление о причинах продления).

5.2. Персональные данные хранятся в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Исключение - случаи, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных.

5.3. Персональные данные на бумажных носителях хранятся в Обществе в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации", Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Приказом Росархива от 20.12.2019 N 236)).

5.4. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

## 6. Порядок блокирования и уничтожения персональных данных

6.1. Общество блокирует персональные данные в порядке и на условиях, предусмотренных законодательством в области персональных данных.

6.2. При достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей персональные данные уничтожаются либо обезличиваются. Исключение может предусматривать федеральный закон.

6.3. Незаконно полученные персональные данные или те, которые не являются необходимыми для цели обработки, уничтожаются в течение семи рабочих дней со дня представления субъектом персональных данных (его представителем) подтверждающих сведений.

6.4. Персональные данные, обработка которых прекращена из-за ее неправомерности и правомерность обработки которых невозможно обеспечить, уничтожаются в течение 10 рабочих дней с даты выявления факта неправомерной обработки.

6.5. Персональные данные уничтожаются в течение 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иным соглашением между ним и Обществом либо если Общество не вправе обрабатывать персональные данные без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6.5.1. При достижении максимальных сроков хранения документов, содержащих персональные данные, персональные данные уничтожаются в течение 30 дней.

6.6. Персональные данные уничтожаются (если их сохранение не требуется для целей обработки персональных данных) в течение 30 дней с даты поступления отзыва субъектом персональных данных согласия на их обработку. Иное может предусматривать договор, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иное соглашение между ним и Обществом. Кроме того, персональные данные уничтожаются в указанный срок, если Общество не вправе обрабатывать их без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6.7. Отбор материальных носителей (документы, жесткие диски, флеш-накопители и т.п.) и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению, осуществляют подразделения Общества, обрабатывающие персональные данные.

6.8. Уничтожение персональных данных осуществляет комиссия, созданная приказом генерального директора.

6.8.1. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

6.8.2. Персональные данные на бумажных носителях уничтожаются с использованием shreddera. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

6.8.3. Комиссия подтверждает уничтожение персональных данных, указанных в п. п. 6.4, 6.5, 6.6 Положения, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденным Приказом Роскомнадзора от 28.10.2022 N 179, а именно:

- актом об уничтожении персональных данных - если данные обрабатываются без использования средств автоматизации;
- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных - если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, которые должны содержаться в указанных документах, утверждаются приказом генерального директора.

6.8.4. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

6.8.5. Уничтожение персональных данных, не указанных в п. 6.8.3 Положения, подтверждается актом, который оформляется непосредственно после уничтожения таких данных. Форма акта утверждается приказом генерального директора.

## 7. Защита персональных данных. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений

7.1. Без письменного согласия субъекта персональных данных Общество не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

7.1.1. Запрещено раскрывать и распространять персональные данные субъектов персональных данных по телефону.

7.2. С целью защиты персональных данных в Обществе приказами генерального директора назначаются (утверждаются):

- работник, ответственный за организацию обработки персональных данных;
- перечень должностей, при замещении которых обрабатываются персональные данные;
- перечень персональных данных, к которым имеют доступ работники, занимающие должности, предусматривающие обработку персональных данных;
- порядок доступа в помещения, в которых ведется обработка персональных данных;
- порядок передачи персональных данных в пределах Общества;
- форма согласия на обработку персональных данных, форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
- порядок защиты персональных данных при их обработке в информационных системах персональных данных;
- порядок проведения внутренних расследований, проверок;

- иные локальные нормативные акты, принятые в соответствии с требованиями законодательства в области персональных данных.

7.3. Работники, которые занимают должности, предусматривающие обработку персональных данных, допускаются к ней после подписания обязательства об их неразглашении.

7.4. Материальные носители персональных данных хранятся в шкафах, запирающихся на ключ. Помещения Общества, в которых они размещаются, оборудуются запирающими устройствами.

7.5. Доступ к персональной информации, содержащейся в информационных системах Общества, осуществляется по индивидуальным паролям.

7.6. В Обществе используется сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

7.7. Работники Общества, обрабатывающие персональные данные, периодически проходят обучение требованиям законодательства в области персональных данных.

7.8. В должностные инструкции работников Общества, обрабатывающих персональные данные, включаются, в частности, положения о необходимости сообщать о любых случаях несанкционированного доступа к персональным данным.

7.9. В Обществе проводятся внутренние расследования в следующих ситуациях:

- при неправомерной или случайной передаче (предоставлении, распространении, доступе) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- в иных случаях, предусмотренных законодательством в области персональных данных.

7.10. Работник, ответственный за организацию обработки персональных данных, осуществляет внутренний контроль:

- за соблюдением работниками, уполномоченными на обработку персональных данных, требований законодательства в области персональных данных, локальных нормативных актов;
- соответствием указанных актов требованиям законодательства в области персональных данных.

Внутренний контроль проходит в виде внутренних проверок.

7.10.1. Внутренние плановые проверки осуществляются на основании ежегодного плана, который утверждается генеральным директором.

7.10.2. Внутренние внеплановые проверки осуществляются по решению работника, ответственного за организацию обработки персональных данных. Основанием для них служит информация о нарушении законодательства в области персональных данных, поступившая в устном или письменном виде.

7.10.3. По итогам внутренней проверки оформляется докладная записка на имя генерального директора. Если выявлены нарушения, в документе приводится перечень мероприятий по их устранению и соответствующие сроки.

7.11. Внутреннее расследование проводится, если выявлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных (далее - инцидент).

7.11.1. В случае инцидента Общество в течение 24 часов уведомляет Роскомнадзор:

- об инциденте;
- его предполагаемых причинах и вреде, причиненном правам субъекта (нескольким субъектам) персональных данных;
- принятых мерах по устранению последствий инцидента;
- представителе Общества, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

При направлении уведомления нужно руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными Приказом Роскомнадзора от 14.11.2022 N 187.

7.11.2. В течение 72 часов Общество обязано сделать следующее:

- уведомить Роскомнадзор о результатах внутреннего расследования;
- предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии).

При направлении уведомления также необходимо руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными Приказом Роскомнадзора от 14.11.2022 N 187.

7.12. В случае предоставления субъектом персональных данных (его представителем) подтвержденной информации о том, что персональные данные являются неполными, неточными или неактуальными, в них вносятся изменения в течение семи рабочих дней. Общество уведомляет в письменном виде субъекта персональных данных (его представителя) о внесенных изменениях и сообщает (по электронной почте) о них третьим лицам, которым были переданы персональные данные.

7.13. Общество уведомляет субъекта персональных данных (его представителя) об устранении нарушений в части неправомерной обработки персональных данных. Уведомляется также Роскомнадзор, если он направил обращение субъекта персональных данных (его представителя) либо сам сделал запрос.

7.13.1. В случае уничтожения персональных данных, которые обрабатывались неправомерно, уведомление направляется в соответствии с п. 7.13 Положения.

7.14. В случае уничтожения персональных данных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки, Общество уведомляет субъекта персональных данных (его представителя) о принятых мерах в письменном виде. Общество уведомляет по электронной почте также третьих лиц, которым были переданы такие персональные данные.

#### 8. Ответственность за нарушение норм, регулирующих обработку персональных данных

8.1. Лица, виновные в нарушении положений законодательства РФ в области персональных данных при обработке персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами. Кроме того, они привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

8.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к их защите, установленных Законом о персональных данных, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.