

Утверждено приказом ФГБУ «Санаторий «Красные камни» Управления делами Президента Российской Федерации от 01 марта 2023г. № 21

ПОЛОЖЕНИЕ

о защите, хранении, обработке и передаче персональных данных работников ФГБУ «Санаторий «Красные камни» Управления делами Президента Российской Федерации

1. Общие положения

1.1. Настоящее Положение определяется в соответствии со следующими нормативными правовыми актами:

- Трудовой кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных";
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера";
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Приказ Роскомнадзора от 5 сентября 2013 г. № 996 "Об утверждении требований и методов по обезличиванию персональных данных";
- Федеральный закон от 30.12.2020г. № 519-ФЗ;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»;
- Федеральный закон от 30.12.2015 № 439-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»;
- Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;
- Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об

утверждении требований к материальным носителям биометрических персональных данных и технология хранения таких данных вне информационных систем персональных данных»;

- Приказ Роскомнадзора от 30.05.2017 №94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»;

- Приказ Роскомнадзора от 30.10.2018 № 159 «О внесении изменений в Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.05.2017 № 94»;

- Приказ Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»;

- Приказ Роскомнадзора от 21.06.2021 № 106 «Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором»;

- Постановление Правительства Российской Федерации от 29.06.2021 №1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных».

1.2. Персональные данные Работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного Работника.

1.3. К персональным данным Работника относятся:

- фамилия, имя, отчество;
- дата рождения;
- гражданство;
- номер страхового свидетельства;
- ИНН;
- данные об образовании (реквизиты дипломов/иных документов);
- данные о приобретенных специальностях;
- семейное положение;
- данные о членах семьи (степень родства, Ф. И. О., год рождения, паспортные данные, включая прописку и место рождения);
- фактическое место проживания;
- контактная информация;
- данные о военной обязанности;
- данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т. п.).

1.4. При определении объема и содержания персональных данных работника Работодатель руководствуется настоящим положением, Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

2. Сбор, обработка и защита персональных данных работника

2.1. Все персональные сведения о работнике Работодатель может получить только от него самого.

В случаях, когда Работодатель может получить необходимые персональные данные работника, только у третьего лица, Работодатель должен уведомить об этом работника, и получить от него письменное согласие.

2.2. Работодатель обязан сообщить работнику о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение.

2.3. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях, а также о его членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

2.4. Обработка персональных данных – сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников ФГБУ «Санаторий «Красные камни»

2.5. Обработка персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия Работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.6. Работодатель разрабатывает меры защиты персональных данных работника.

2.7. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

2.8. Персональные данные работника являются конфиденциальной информацией и не могут быть использованы Работодателем или любым иным лицом в личных целях

2.9. Обработка персональных данных работников Работодателем возможна только с письменного согласия работника.

2.10. Письменное согласие работника на обработку своих персональных данных должно включать:

- 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.

- 2.11. Согласие работника не требуется, если:
- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона;
 - обработка персональных данных осуществляется в целях исполнения трудового договора;
 - обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
 - персональные данные являются общедоступными;
 - персональные данные относятся к состоянию здоровья Работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;
 - персональные данные обрабатываются по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

2.12. Оператор, допустивший утечку персональных данных, обязан в течение 24 часов сообщить об этом в Роскомнадзор, а в течение 72 часов предоставить в ведомство результаты внутреннего расследования инцидента с указанием причины и виновных лиц.

2.13. Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя, в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя.

3. Передача и хранение персональных данных работника

- 3.1. При передаче персональных данных работника Работодатель должен соблюдать следующие требования:
- не сообщать персональные данные работника третьей стороне без их письменного согласия, за исключением случаев, установленных федеральным законом;
 - не сообщать персональные данные работника в коммерческих целях без их письменного согласия;
 - обработка персональных данных работника 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;
 - предупредить лиц, получивших персональные данные работника, 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, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности);
 - осуществлять передачу персональных данных работника в пределах ФГБУ «Санаторий «Красные камни» в соответствии с настоящим Положением;
 - разрешать доступ к персональным данным работника только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции;
 - не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой

6.3 Внутренняя защита:

6.3.1 Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

- Ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данным сотрудников.
- Строгое избирательное и обоснованное распределение документов и информации между работниками;
- Рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- Знание работниками требований нормативно-методических документов по защите информации и сохранения тайны;
- Наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- Определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- Организация порядка уничтожения информации;
- Своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- Воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

6.3.2 Защита персональных данных пациентов на электронных носителях. Все документы, содержащие персональные данные пациента, должны иметь ограниченный доступ.

6.4 Внешняя защита:

6.4.1 Для обеспечения внешней защиты персональных данных пациентов необходимо соблюдать ряд мер:

- Порядок приема, учета и контроля деятельности посетителей;
- Технические средства охраны (электронный ключ, сигнализации);
- Порядок охраны территории, зданий, помещений.

6.5 Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны не разглашать персональные данные пациентов.

6.6 Кроме мер защиты персональных данных, установленных законодательством, Санаторий, сотрудники Санатория, пациенты и их представители могут выработать совместные меры защиты персональных данных пациентов.

6.7 Оператор, допустивший утечку персональных данных, обязан в течение 24 часов сообщить об этом в Роскомнадзор, а в течение 72 часов предоставить в ведомство результаты внутреннего расследования инцидента с указанием причины и виновных лиц.

6.8 Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъектов персональных данных или его представителя, в течение десяти рабочих дней с момента получения запроса субъекта персональных данных или его представителя.

7. ПРАВА И ОБЯЗАННОСТИ ПАЦИЕНТОВ

7.1 В целях защиты персональных данных, хранящихся в Санатории, пациент имеет право:

- Требовать исключения или исправления неверных или неполных данных;
- Получать доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, только с письменного заявления на имя директора Санатория;

4.3. Работодатель обязан ознакомить работника и его представителей с настоящим Положением и их правами в области защиты персональных данных под роспись.

4.4. Работодатель обязан обеспечить работнику свободный бесплатный доступ к его персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законом.

4.5. Работодатель обязан по требованию работника предоставить полную информацию о его персональных данных и обработке этих данных.

4.6. Работодатель обязан ежегодно под роспись знакомить работника с записями в личной карточке Т-2.

5. Права работника на защиту персональных данных

5.1. Работник в целях обеспечения защиты своих персональных данных, хранящихся у Работодателя, имеет право 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. Работник вправе получать доступ к своим персональным данным и знакомиться с ними, а также получать копии любой записи, содержащей персональные данные.

5.3. Работник может требовать от Работодателя уточнить, исключить или исправить неполные, неверные, устаревшие, недостоверные, незаконно полученные или не являющиеся необходимыми для Работодателя персональные данные.

5.4. Работник вправе требовать от Работодателя извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.5. Если работник считает, что Работодатель осуществляет обработку его персональных данных с нарушением требований Федерального закона или иным образом нарушает их права и свободы, он вправе обжаловать действия или бездействие Работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

6. Порядок уничтожения, блокирования персональных данных

6.1. В случае выявления неправомерной обработки персональных данных при обращении работника, Работодатель обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту, с момента такого обращения.

6.2. В случае выявления неточных персональных данных при обращении работника, Работодатель обязан осуществить блокирование персональных данных, относящихся к этому субъекту, с момента такого обращения, если блокирование

персональных данных не нарушает права и законные интересы субъекта или третьих лиц.

6.3. В случае подтверждения факта неточности персональных данных, Работодатель на основании сведений, представленных работником, иных необходимых документов обязан уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

6.4. В случае выявления неправомерной обработки персональных данных, осуществляемой Работодателем, Работодатель в срок, не превышающий трех рабочих дней с момента этого выявления, обязан прекратить неправомерную обработку персональных данных.

6.5. Если обеспечить правомерность обработки персональных данных невозможно, Работодатель в срок, не превышающий десяти рабочих дней с момента выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

6.6. Об устранении допущенных нарушений или об уничтожении персональных данных Работодатель обязан уведомить работника.

6.7. В случае достижения цели обработки персональных данных Работодатель обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с момента достижения цели обработки персональных данных, если иное не предусмотрено трудовым договором.

6.8. В случае отзыва Работником согласия на обработку его персональных данных Работодатель обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с момента поступления указанного отзыва, если иное не предусмотрено трудовым договором.

6.9. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.4-6.8 настоящего Положения, Работодатель осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

7.1. Работники ФГБУ «Санаторий «Красные камни», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами

7.2. Моральный вред, причиненный Работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных Работником убытков.

8. Заключительные положения

8.1. Настоящее Положение вступает в силу с момента его утверждения директором ФГБУ «Санаторий «Красные камни» и действует бессрочно, до замены его новым Положением.

8.2. Все изменения в Положение вносятся приказом директора ФГБУ «Санаторий «Красные камни».

8.3. Все работники ФГБУ «Санаторий «Красные камни» должны быть ознакомлены с настоящим Положением под роспись.