

УТВЕРЖДАЮ

Исполняющий обязанности
Главного врача
ГБУЗ Республики Мордовия
«КДС «Сосновый бор»

_____ Л.А. Семикова
Приказ № 25 от 31.08.2022 г.

ПОЛИТИКА

**оператора в отношении обработки персональных данных в информационных
системах Государственного бюджетного учреждения здравоохранения
Республики Мордовия «Ковылкинский детский санаторий «Сосновый бор»**

СОДЕРЖАНИЕ

1. Термины и определения.....	3
2. Общие положения.....	4
3. Правовые основы обработки персональных данных.....	4
4. Принципы обработки персональных данных.....	5
5. Права субъектов персональных данных.....	8
6. Меры по обеспечению безопасности персональных данных.....	8
7. Заключение.....	9

1. Термины и определения

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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.

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

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

2. Общие положения

2.1. Настоящий документ определяет политику Государственного бюджетного учреждения здравоохранения Республики Мордовия «Ковылкинский детский санаторий «Сосновый бор» (далее – Учреждение) в отношении обработки персональных данных (далее – Политика) и меры по обеспечению безопасности персональных данных с целью защиты прав и свобод человека и гражданина при обработке его персональных данных. Политика разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными федеральными законами и нормативно-правовыми актами.

2.2. Настоящая политика характеризуется следующими признаками:

- раскрывает способы и принципы обработки персональных данных, права и обязанности Учреждения при обработке персональных данных, права субъектов персональных данных, а также включает требования, реализуемые Учреждением в целях обеспечения безопасности персональных данных при их обработке.
- является общедоступным документом, декларирующим концептуальные основы деятельности Учреждения при обработке и защите персональных данных.

3. Правовые основы обработки персональных данных

3.1. Политика обработки персональных данных в Учреждении 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 Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- 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 ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности 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»;

– Иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

3.2. Во исполнение настоящей Политики Учреждения утверждены следующие локальные нормативные правовые акты:

- Перечень информационных ресурсов, подлежащих защите.
- Перечень информационных систем.
- Перечень работников, допущенных к работе с персональными данными.
- Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- Акты классификации информационных систем.
- Акты оценки возможного вреда субъектам ПДн.
- Акты формирования итогового набора мер защиты информации.
- Инструкции по работе с ПДн.

4. Принципы обработки персональных данных

4.1. Учреждение, являясь оператором персональных данных, осуществляет обработку персональных данных работников Учреждения и других субъектов персональных данных, не состоящих с Учреждением в трудовых отношениях.

4.2. Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:

- законности и справедливой основы;
- ограничения обработки персональных данных достижением конкретных, заранее определённых и законных целей;
- недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;
- недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработки только тех персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объёма обрабатываемых персональных данных заявленным целям обработки;
- недопущения обработки избыточных персональных данных по отношению к заявленным целям их обработки;
- обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;
- уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.3. Персональные данные обрабатываются в Учреждении в следующих целях:

- осуществление медицинской деятельности;
- осуществление образовательной деятельности;
- ведение и автоматизация бухгалтерского учета;
- ведение и автоматизация кадрового учета.

4.3.1. Учреждением при осуществлении медицинской деятельности обрабатываются следующие персональные данные:

- 1) Фамилия, Имя, Отчество;
- 2) Адрес регистрации и фактического проживания;
- 3) Дата и место рождения;
- 4) Номер и серия паспорта, кем и когда выдан;
- 5) Свидетельство о рождении;
- 6) Полис обязательного медицинского страхования (ОМС);
- 7) Рост, вес, пол;
- 8) Номер телефона.
- 9) Состояние здоровья – специальная категория персональных данных.

Субъектами персональных данных чьи данные подлежат обработке при осуществлении Учреждением медицинской деятельности являются лица получающие путевки на санаторно-курортное лечение медицинскими организациями и лица имеющие намерение заключить договор на оказание платных медицинских услуг.

4.3.2. Учреждением при осуществлении образовательной деятельности обрабатываются следующие персональные данные:

- 1) Фамилия, Имя, Отчество;
- 2) Адрес регистрации и фактического проживания;
- 3) Дата и место рождения;
- 4) Номер и серия паспорта, кем и когда выдан;
- 5) Свидетельство о рождении;
- 6) Номер телефона.

Субъектами персональных данных чьи данные подлежат обработке при осуществлении Учреждением образовательной деятельности являются лица получающие путевки на санаторно-курортное лечение.

4.3.3. При ведении и автоматизации бухгалтерского учета Учреждением обрабатываются следующие персональные данные:

- 1) Фамилия, Имя, Отчество;
- 2) Адрес регистрации и фактического проживания;
- 3) Дата и место рождения;
- 4) Номер и серия паспорта, кем и когда выдан;
- 5) Свидетельство о рождении ребенка;
- 6) Идентификационный номер налогоплательщика (ИНН);
- 7) Страховой номер индивидуального лицевого счета (СНИЛС);
- 8) Сведения о доходах с прежнего места работы;
- 9) Номер телефона.

Субъектами персональных данных чьи данные подлежат обработке при

ведении и автоматизации бухгалтерского учета являются лица, состоящие в трудовых отношениях с Учреждением.

4.3.4. При ведении и автоматизации кадрового учета Учреждением обрабатываются следующие персональные данные:

- 1) Фамилия, Имя, Отчество;
- 2) Адрес регистрации и фактического проживания;
- 3) Дата и место рождения;
- 4) Номер и серия паспорта, кем и когда выдан;
- 5) Свидетельство о заключении брака;
- 6) Свидетельство о рождении ребенка;
- 7) Идентификационный номер налогоплательщика (ИНН);
- 8) Страховой номер индивидуального лицевого счета (СНИЛС);
- 9) Сведения о доходах с прежнего места работы;
- 10) Номер телефона;
- 11) Документ воинского учета;
- 12) Документ об образовании;
- 13) Сведения о трудовом стаже;
- 14) Справка о наличии (отсутствии) судимости.

Субъектами персональных данных чьи данные подлежат обработке при ведении и автоматизации кадрового учета являются лица, вступающие в трудовые отношения с Учреждением.

4.4. Обработка персональных данных в Учреждении при реализации вышеуказанных целей осуществляется следующими способами:

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

Персональные данные граждан хранятся на бумажных носителях и в электронном виде.

Ответственные лица за хранение документов, содержащих персональные данные граждан, назначены приказом Исполняющего обязанности Главного врача от «31» августа 2022 г. № 23 «О защите персональных данных».

Хранение окончанных производством документов, содержащих персональные данные граждан, осуществляется в помещениях Учреждения, предназначенных для хранения обработанной документации.

Ответственные лица за хранение окончанных производством документов, содержащих персональные данные граждан, назначаются приказом Исполняющего обязанности Главного врача от «31» августа 2022 г. № 23 «О защите персональных данных».

Возможна передача персональных данных граждан по внутренней сети организации с использованием технических и программных средств защиты информации, с доступом только для работников Учреждения, допущенных к работе с персональными данными граждан приказом Исполняющего обязанности Главного врача от «31» августа 2022 г. № 23 «О защите персональных данных» и

только в объеме, необходимом данным работникам для выполнения своих должностных обязанностей.

Обработка и хранение персональных данных граждан осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Хранение документов, содержащих персональные данные граждан, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов.

5. Права субъектов персональных данных

5.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Учреждением.

5.2. Субъект персональных данных вправе требовать от Учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

5.4. Для реализации и защиты своих прав и законных интересов субъект персональных данных имеет право обратиться в Учреждение. Учреждение рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

5.5. Субъект персональных данных вправе обжаловать действия или бездействие Учреждения путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

5.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

6. Меры по обеспечению безопасности персональных данных

6.1. Учреждение при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

- назначением ответственного лица за организацию обработки и обеспечение безопасности персональных данных в Учреждении.
- принятием локальных нормативных актов и иных документов в области обработки и защиты персональных данных.
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.
- осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам Учреждения.
- ознакомлением работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных и/или обучением указанных сотрудников.
- выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.
- контролем над принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.
- иными мерами, предусмотренными законодательством Российской Федерации в области персональных данных.

6.2. Учреждение обеспечивает взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

6.3. Указанная в п. 6.2. информация (за исключением информации, составляющей государственную тайну) передается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в уполномоченный орган по защите прав субъектов персональных данных.

7. Заключение

7.1. Настоящая Политика является внутренним документом Учреждения, общедоступной и подлежит размещению на официальном сайте Учреждения.

7.2. Настоящая Политика подлежит изменению, дополнению в случае принятия новых Федеральных законов и иных нормативных правовых актов в области обработки и защиты персональных данных.

7.3. Ответственность работников Учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих

обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации.

Программист _____ Е.Н. Волков

«__» _____ 2022 г.