Приложение 9

|  |
| --- |
| **У Т В Е Р Ж Д Е Н О** |
| приказом главного врача ГБУЗ Республики Мордовия «Детская поликлиника № 2» |
| от «17» июня 2021 г. № 231 |

**политика**

**оператора в отношении обработки персональных данных в информационных системахГБУЗ Республики Мордовия**

 **«Детская поликлиника № 2»**

**СОДЕРЖАНИЕ**

[1. Термины и определения 3](#_Toc528680021)

[2. Общие положения 4](#_Toc528680022)

[3. Правовые основы обработки персональных данных 4](#_Toc528680023)

[4. Принципы обработки персональных данных 5](#_Toc528680024)

[5. Права субъектов персональных данных 6](#_Toc528680025)

[6. Меры по обеспечению безопасности персональных данных 6](#_Toc528680026)

[7. Заключение 8](#_Toc528680027)

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.

1. **Общие положения**
	1. Настоящийдокумент определяет политику ГБУЗ Республики Мордовия «Детская поликлиника №2»(далее –(Организация)) 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 июля2006 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. Настоящая политика характеризуется следующими признаками:
* раскрывает способы и принципы обработки персональных данных, права и обязанности (Организации) при обработке персональных данных, права субъектов персональных данных, а также включает требования, реализуемые (Организация)м в целях обеспечения безопасности персональных данных при их обработке.
* является общедоступным документом, декларирующим концептуальные основы деятельности (Организации) при обработке и защите персональных данных.
1. **Правовые основы обработки персональных данных**
	1. Политика обработки персональных данных в (Организации)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.
	1. Во исполнение настоящей Политики (Организации) 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.
* Актыформирования итогового набора мер защиты информации.
* Инструкции по работе с ПДн.
1. **Принципы обработки персональных данных**
	1. (Организация), являясь оператором персональных данных, осуществляет обработку персональных данных работников (Организации) и других субъектов персональных данных, не состоящих с(Организация) в трудовых отношениях.
	2. Обработка персональных данных в (Организации) 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.
	1. Персональные данные обрабатываются в (Организации)в следующих целях:

‒ осуществление образовательной деятельности;

‒ ведение и автоматизация кадрового учета;

‒ автоматизация основных и вспомогательных учебно-воспитательных процессов в образовательном учреждении.

* 1. Обработка персональных данных в (Организации) осуществляется следующими способами:
* неавтоматизированная обработка персональных данных;
* автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям;
* смешанная обработка персональных данных.
1. **Права субъектов персональных данных**
	1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных (Организация)м.
	2. Субъект персональных данных вправе требовать от (Организации) 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.
	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.
	4. Для реализации и защиты своих прав и законных интересов субъект персональных данных имеет право обратиться в (Организации). (Организация) 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. Субъект персональных данных вправе обжаловать действия или бездействие (Организации) путем обращения в уполномоченный орган по защите прав субъектов персональных данных.
	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.
2. **Меры по обеспечению безопасности персональных данных**
	1. (Организация) 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 (Организации).
* 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 27июля 2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам (Организации).
* ознакомлением работников (Организации), 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.
* иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.
1. **Заключение**
	1. Настоящая Политика является внутренним документом (Организации), общедоступной и подлежит размещению на официальном сайте (Организации).
	2. Настоящая Политика подлежит изменению, дополнению в случае принятия новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.
	3. Ответственность работников (Организации), имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российский Федерации.