

УТВЕРЖДЕНО
Приказом
федерального государственного бюджетного
учреждения «Детский медицинский центр»
Управления делами Президента Российской Федерации

от «20» 01 № 48 . 2023

Дата ввода в действие
«20» 01 . 2023

Политика информационной безопасности в отношении обработки персональных данных в
федеральном государственном бюджетном учреждении «Детский медицинский центр»

Редакция №3

1. Определения

1.1. В настоящем документе (далее - Политика) используются следующие термины и их определения:

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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;

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 (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

оператор – федеральное государственное бюджетное учреждение «Детский медицинский центр», 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;

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

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

2. Общие положения

2.1. Политика разработана в соответствии с Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 года №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами,

- операторами, являющимися государственными или муниципальными органами».
- 2.2. Политика является общедоступным документом, декларирующим основы деятельности федерального государственного бюджетного учреждения «Детский медицинский центр», связанной с обработкой персональных данных.
 - 2.3. Политика не распространяется на: а) организацию хранения, комплектования, учета и использования содержащих персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации; б) обработку персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.
 - 2.4. Федеральное государственное бюджетное учреждение «Детский медицинский центр» является оператором, организующим и осуществляющим обработку персональных данных, определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
3. Принципы и цели обработки персональных данных
- 3.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.
 - 3.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
 - 3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
 - 3.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
 - 3.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточны по отношению к заявленным целям их обработки.
 - 3.6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры или обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
 - 3.7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

- 3.8.Целью Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
- 3.9.Целями обработки персональных данных являются: а) обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011 г №323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. №61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 года №326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. №1006; б) осуществление прав и обязанностей в соответствии с трудовым законодательством; в) выполнение обязательств по гражданско-правовым договорам (контрактам) и иным соглашениям.
4. Состав и субъекты персональных данных
- 4.1.В федеральном государственном бюджетном учреждении «Детский медицинский центр» осуществляется обработка следующих персональных данных: а) данные полученные при осуществлении трудовых отношений; б) данные полученные для осуществления отбора кандидатов/соискателей на вакантные должности; в) данные полученные при осуществлении гражданско-правовых отношений; г) данные полученные при оказании медицинской помощи. Полный список обрабатываемых персональных данных представлен в Перечне персональных данных, утвержденном директором федерального государственного бюджетного учреждения «Детский медицинский центр».
- 4.2.Субъектами обработки персональных данных являются: а) физические лица, состоящие с федеральным государственным бюджетным учреждением «Детский медицинский центр» в отношениях, регулируемых трудовым законодательством; б) физические лица, являющие близкими родственниками сотрудников федерального государственного бюджетного учреждения «Детский медицинский центр»; в) физические лица, уволившиеся из федерального государственного бюджетного учреждения «Детский медицинский центр»; г) физические лица, являющиеся кандидатами/соискателями на замещение вакантных должностей федерального государственного бюджетного учреждения «Детский медицинский центр»; д) физические лица, состоящие с федеральным государственным бюджетным учреждением «Детский медицинский центр» в гражданско-правовых отношениях; е) физические лица, обратившиеся в федеральное государственное бюджетное учреждение «Детский медицинский центр» за медицинской помощью.
- 4.3.Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей: а) подтверждение факта обработки персональных данных; б) правовые основания и цели обработки персональных данных; в) применяемые способы обработки

персональных данных; г) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом; д) сроки обработки персональных данных, в том числе сроки их хранения; е) иные сведения, предусмотренные №152-ФЗ «О персональных данных».

4.4.Субъект персональных данных вправе требовать уточнения его персональных данных, их блокировки или уничтожения в случае, если его персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.5.Субъект персональных данных, считающий, что обработка его персональных данных осуществляется с нарушением требований №152-ФЗ «О персональных данных» или нарушаются его права и свободы иным образом, вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций — Роскомнадзор) или в судебном порядке.

5. Обработка персональных данных

5.1.Обработка персональных данных в федеральном государственном бюджетном учреждении «Детский медицинский центр» осуществляется при соблюдении одного из перечисленных условий: а) с согласия субъекта персональных данных на обработку его персональных данных; б) необходимости достижения целей, предусмотренных международным договором Российской Федерации; в) необходимости осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве; г) с согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения (доступа неограниченного круга лиц); д) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом; е) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

5.2.Обработка персональных данных осуществляется с использованием и без использования (на бумажном носителе) средств автоматизации.

5.3.Федеральное государственное бюджетное учреждение «Детский медицинский центр» не осуществляет передачу персональных данных через государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства

6. Обязанности Оператора при обработке персональных данных

6.1.Издавать локальные нормативные правовые акты по вопросам обработки персональных данных, а также локальные нормативные правовые акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации и иных нормативных

- правовых актов, связанных с обработкой персональных данных, устранение последствий таких нарушений.
- 6.2. Определять состав и перечень правовых, организационных и технических мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами и осуществлять их применение.
 - 6.3. Назначать лицо, ответственное за организацию обработки персональных данных.
 - 6.4. Осуществлять внутренний контроль над соблюдением законодательства Российской Федерации и иных нормативных правовых актов о персональных данных, в том числе требований к защите персональных данных.
 - 6.5. Обеспечивать доведение до сведения сотрудников положений законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.
 - 6.6. Организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль над приемом и обработкой таких обращений и запросов.
 - 6.7. Обеспечивать выполнение лицами, осуществляющими обработку персональных данных, и лицами, имеющими доступ к персональным данным, требований по защите персональных данных, установленных нормативными правовыми актами.
 - 6.8. Обеспечивать конфиденциальность обрабатываемых персональных данных, кроме персональных данных, разрешенных к доступу неограниченному кругу лиц, если иное не предусмотрено федеральным законом.
 - 6.9. Принимать меры по обеспечению безопасности персональных данных при их обработке.
 - 6.10. Не допускать обработку и приобщение к личному делу субъекта персональных данных сведений расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, членства в общественных объединениях или его профсоюзной деятельности, если иное не предусмотрено федеральным законом.
 - 6.11. Обеспечивать уничтожение персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
 - 6.12. Опубликовать или иным образом обеспечить неограниченный доступ к данному документу и к сведениям о реализуемых требованиях к защите персональных данных.
 - 6.13. Выполнять иные обязанности оператора, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.
7. Порядок доступа к персональным данным и их предоставления
 - 7.1. К обработке персональных данных допускаются сотрудники федерального государственного бюджетного учреждения «Детский медицинский центр», выполняющие соответствующие функции по предоставлению услуг, реализации служебных полномочий.
 - 7.2. Лицам, допущенным к обработке персональных данных, предоставляется доступ только к персональным данным, необходимым для выполнения их служебных обязанностей в пределах возложенных соответствующих задач и функций.

- 7.3. Каждое лицо, допущенное к обработке персональных данных, использует индивидуальную учетную запись, которую не имеет права передавать другим лицам.
- 7.4. Оператор вправе передавать (предоставлять) персональные данные третьим лицам с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
- 7.5. Основанием для отказа в предоставлении персональных данных третьим лицам являются: а) отсутствие согласия субъекта персональных данных; б) отсутствие условий, предусмотренных №152-ФЗ «О персональных данных», при которых согласие субъекта персональных данных не требуется.
8. Организация защиты персональных данных
- 8.1. Персональные данные относятся к сведениям ограниченного доступа и подлежат защите.
- 8.2. При организации защиты персональных данных при их обработке федеральное государственное бюджетное учреждение «Детский медицинский центр» руководствуется, в том числе: а) Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»; б) постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; в) постановлением Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»; г) постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- 8.3. Под безопасностью информации понимают состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.
- 8.4. Безопасность информации, обрабатываемой в федеральном государственном бюджетном учреждении «Детский медицинский центр» достигается: а) комплексом действий, направленных на решение проблемы защиты информационной среды в рамках учреждения; б) управления рисками, связанными с разглашением информации или влиянием на аппаратные и программные модули защиты.
- 8.5. Задачами системы защиты персональных данных являются исключение или минимизация ущерба от возможной реализации случайных или злонамеренных воздействий на персональные данные, а также прогнозирование и предотвращение таких воздействий.
- 8.6. Меры, принимаемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, подразделяются на правовые, организационные и технические
- 8.7. К правовым мерам защиты персональных данных относится принятие правовых актов, в соответствии с федеральными законами в области защиты персональных данных и принятыми в их исполнение нормативными документами, закрепляющих права и обязанности субъектов информационных

отношений в процессе обработки персональных данных, а также устанавливающих ответственность за нарушение этих правил.

- 8.8. Организационные меры защиты персональных данных: а) назначение ответственных за обеспечение безопасности информации; б) разработка и поддержание в актуальном состоянии организационно-распорядительных документов, регламентирующих порядок обработки персональных данных, создания и функционирования системы защиты персональных данных; в) информирование лиц, осуществляющих обработку персональных данных, о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки; г) осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и безопасности персональных данных в федеральном государственном бюджетном учреждении «Детский медицинский центр» требованиям законодательства Российской Федерации и иных нормативных правовых актов о персональных данных, в том числе требованиям к защите персональных данных; д) обучение и повышение квалификации сотрудников, ответственных за организацию обработки и обеспечение безопасности информации.
- 8.9. К техническим мерам защиты относится использование программно-аппаратных средств, выполняющих самостоятельно или в комплексе с другими средствами функции защиты персональных данных, и методов защиты, в том числе: а) программной или программно-технической защиты от несанкционированного доступа к информационным ресурсам автоматизированных рабочих мест, на которых обрабатываются персональные данные; б) средств защиты от вредоносного программного обеспечения; в) обеспечение раздельной фиксации на материальных носителях персональных данных, имеющих различную цель обработки, или их раздельной обработки; г) обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
- 8.10. Федеральным государственным бюджетным учреждением «Детский медицинский центр» применяются сертифицированные средства защиты информации, соответствующие требованиям, установленным уполномоченными органами в области технической защиты информации.
- 8.11. Лица, ответственные за организацию обработки персональных данных, при обеспечении безопасности персональных данных вправе, в том числе: а) иметь доступ к информации, касающейся обработки персональных данных; б) привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых Оператором, сотрудников с возложением на них соответствующих обязанностей и закреплением ответственности.
9. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных
- 9.1. Лица, виновные в нарушении требований по организации обработки персональных данных в федеральном государственном бюджетном учреждении «Детский медицинский центр» несут ответственность за ненадлежащее выполнение возложенных функций по организации обработки персональных данных в соответствии с законодательством Российской Федерации и иными нормативными правовыми актами в области персональных данных.
- 9.2. Лица, осуществляющие обработку персональных данных в федеральном государственном бюджетном учреждении «Детский медицинский центр» в соответствии со своими полномочиями, несут гражданско-правовую,

уголовную, административную, дисциплинарную ответственность за нарушение требований к обработке и защите персональных данных, предусмотренную законодательством Российской Федерации.