

УТВЕРЖДАЮ
Главный врач ГБУЗ КО
"Балтийская центральная районная
больница"

В. М. Пикалов

«31» января 2023



**Политика
обработки и защиты персональных данных**

г. Балтийск
2023 г.

1. Определения и сокращения, используемые в Политике

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

1.2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств информатизации 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.

1.3. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

1.5. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.6. 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.

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

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

1.9. Информация – сведения (сообщения, данные) независимо от формы их представления.

2. Общие положения

2.1. Настоящий документ определяет политику государственного бюджетного учреждения здравоохранения Калининградской области "Балтийская центральная районная больница" (далее – Оператор) в отношении обработки и защиты персональных данных.

2.2. Политика обработки и защиты персональных данных Оператора (далее – Политика) определяет:

- правовые основания обработки персональных данных;
- принципы и цели обработки персональных данных;
- перечни субъектов персональных данных и обрабатываемых персональных данных;
- операции, совершаемые с персональными данными, и сроки их обработки;
- права и обязанности субъектов и работников Оператора при обработке персональных данных;
- меры, принимаемые Оператора для защиты персональных данных;
- контроль и надзор за обработкой персональных данных.

2.3. Настоящая Политика разработана в соответствии с п. 1 и п. 2 ст. 18.1 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» и с учетом требований Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации в области персональных данных.

2.4. Целью настоящей Политики является определение порядка обработки персональных данных граждан; 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, а также установление ответственности должностных лиц, имеющих доступ к персональным данным граждан, за невыполнение требований и норм, регулирующих порядок обработки и защиты персональных данных.

2.5. Политика действует в отношении всех персональных данных, обрабатываемых Оператором, полученных как до, так и после утверждения настоящей Политики.

2.6. Действие настоящей Политики распространяется на персональные данные, обрабатываемые с применением средств автоматизации и без применения таких средств.

2.7. Действие настоящей Политики распространяется на все процессы, в рамках которых осуществляется обработка персональных данных субъектов персональных данных всех категорий, а также на должностных лиц, принимающих участие в указанных процессах.

2.8. Основные положения документа могут быть распространены также на подразделения других организаций и учреждений, осуществляющие взаимодействие с Оператором в качестве поставщиков и потребителей (пользователей) информации.

3. Правовые основания обработки персональных данных

3.1. Правовыми основаниями обработки Оператором персональных данных являются:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 29 декабря 2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;
- Федеральный закон от 22 октября 2004 г. №125-ФЗ «Об архивном деле в Российской Федерации»;
- Постановление Госкомстата Российской Федерации «Об утверждении унифицированных форм первичной учетной документации по учету труда и оплаты» №1 от 05.01.2004 г.;
- Приказ Министерства здравоохранения СССР от 4 октября 1980 г. №1030 «Об утверждении форм первичной медицинской документации учреждений здравоохранения»;
- Устав Оператора;
- Договор или контракт между Оператором и субъектом персональных данных;
- Согласие субъекта персональных данных на обработку его персональных данных.

4. Персональные данные, обрабатываемые Оператором

4.1. Оператором обрабатываются персональные данные следующих категорий субъектов:

- Работники.
- Близкие родственники работников.

- Уволенные работники.
- Кандидаты на вакантную должность.
- Пациенты.
- Законные представители пациентов.
- Контрагенты.

4.2. Перечень персональных данных работников, близких родственников работников, уволенных работников, кандидатов на вакантную должность:

- фамилия, имя, отчество;
- дата рождения и место рождения;
- паспортные данные (серия, номер, когда и кем выдан, код подразделения);
- адрес постоянной регистрации и проживания;
- гражданство;
- пол;
- номер контактного телефона;
- семейное положение;
- сведения о местах обучения, образовании, о повышении квалификации, профессиональной переподготовке, стажировке;
- сведения об ученой степени, ученом звании;
- сведения о наградах, поощрениях, взысканиях;
- специальность, квалификация;
- сведения из свидетельства о постановке на налоговый учет (ИНН);
- сведения из свидетельства о государственном пенсионном страховании (страховой номер);
- сведения о начислениях по заработной плате;
- должность;
- сведения о воинской обязанности;
- данные о трудовом стаже, включая предыдущие места работы;
- данные о налоговых вычетах;
- сведения о льготах;
- сведения о состоянии здоровья;
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;
- фотографическое изображение;
- номер банковского лицевого счета, номер банковской карты, наименование банка;

– состав семьи: степень родства, ФИО, дата рождения, место учебы ребенка, сведения документа, удостоверяющего личность ребенка.

4.3. Перечень персональных данных пациентов, законных представителей пациентов:

- фамилия, имя, отчество;
- пол;
- дата рождения и место рождения;
- адрес регистрации и проживания;
- номер полиса ОМС;
- данные документа удостоверяющего личность (серия, номер, дата выдачи, наименование выдавшего органа, код подразделения);
- СНИЛС;
- сведения о состоянии здоровья;
- диагноз;
- результаты анализов;
- номер контактного телефона;
- место работы.

4.4. Перечень персональных данных контрагентов:

- фамилия, имя, отчество;
- адрес регистрации;
- номер контактного телефона;
- адрес электронной почты;
- сведения из Свидетельства о государственной регистрации физического лица в качестве индивидуального предпринимателя.

5. Операции, совершаемые с персональными данными.

Сроки обработки персональных данных

5.1. Оператор осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.2. Обработка персональных данных осуществляется с момента их получения Оператором и прекращается:

- по достижению целей обработки персональных данных;
- в связи с отсутствием необходимости в достижении заранее заявленных целей обработки персональных данных;
- в связи с отзывом согласия на обработку персональных данных;

– в связи с ликвидацией Оператора как юридического лица.

Срок обработки персональных данных работников – в течение срока действия трудового договора и 75 лет после его окончания, если не установлен иной срок архивного хранения в соответствии с действующим законодательством.

Срок обработки персональных данных близких родственников работников – в течение срока действия трудового договора работника и 75 лет после его окончания, если не установлен иной срок архивного хранения в соответствии с действующим законодательством.

Срок обработки персональных данных уволенных работников – 75 лет после окончания трудового договора, если не установлен иной срок архивного хранения в соответствии с действующим законодательством.

Срок обработки персональных данных кандидатов на вакантную должность – 5 лет после предоставления информации.

Срок обработки персональных данных пациентов – в течение срока оказания медицинского обеспечения и 25 лет после его окончания, если не установлен иной срок архивного хранения в соответствии с действующим законодательством.

Срок обработки персональных данных законных представителей пациентов – в течение срока оказания медицинского обеспечения пациенту и 25 лет после его окончания, если не установлен иной срок архивного хранения в соответствии с действующим законодательством.

Срок обработки персональных данных контрагентов – в течение срока оказания услуг, предусмотренных договором или контрактом между Оператором и контрагентом, и 5 лет после его окончания, если не установлен иной срок архивного хранения в соответствии с действующим законодательством.

6. Цели и принципы обработки персональных данных

6.1. Целями обработки персональных данных Оператором являются:

- обеспечение соблюдения законов или иных правовых актов, содействие в трудоустройстве, обучении и профессиональном продвижении, контроль количества и качества выполняемой работы;
- оказание медицинского обеспечения;
- оказание услуг, предусмотренных договором или контрактом между Оператором и контрагентом.

6.2. Обработка персональных данных осуществляется на основе следующих принципов:

- обработка персональных данных осуществляется на законной основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных целей;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки;
- не допускается обработка избыточных по отношению к заявленным целям персональных данных;
- при обработке персональных данных обеспечиваются их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законодательством или договором, стороной которого является субъект персональных данных.

7. Права субъекта персональных данных

7.1. В соответствии с п.3 ст. 14 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных.

Информация, касающаяся обработки персональных данных субъекта, предоставляемая субъекту, не должна содержать персональных данных, относящихся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких данных.

7.2. Субъект персональных данных вправе требовать от Оператора уточнения 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.

7.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

7.4. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать

действия или бездействие Оператора в Уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда.

8. Конфиденциальность персональных данных

8.1. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных».

9. Получение и передача персональных данных третьим лицам

9.1. Оператор в ходе своей деятельности имеет право получать от третьих лиц и передавать третьим лицам обрабатываемые персональные данные в интересах и с согласия субъектов персональных данных, а также без согласия субъекта персональных данных – в случаях, предусмотренных федеральным законодательством.

10. Общедоступные источники персональных данных

10.1. В целях информационного обеспечения Оператором могут создаваться общедоступные источники персональных данных субъектов персональных данных – работников Оператора, в том числе справочники и адресные книги. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться персональные данные работников.

10.2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных, уполномоченного органа по защите прав субъектов персональных данных либо по решению суда.

11. Поручение обработки персональных данных другому лицу

11.1. Оператор вправе поручить обработку персональных данных другому лицу на основании заключаемого с ним договора, только с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Лицо,

осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» и настоящей Политикой.

12. Права и обязанности лиц, уполномоченных на обработку персональных данных

12.1. Лица, уполномоченные на обработку персональных данных обязаны:

- знать и выполнять требования законодательства в области обеспечения защиты персональных данных;
- хранить в тайне известные им персональные данные, информировать о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;
- соблюдать правила использования персональных данных, порядок их учета и хранения, исключить доступ к ним посторонних лиц;
- обрабатывать только те персональные данные, к которым получен доступ в силу исполнения трудовых обязанностей.

12.2. При обработке персональных данных запрещается:

- использовать сведения, содержащие персональные данные, в личных целях, а также при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;
- передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта) без использования сертифицированных средств криптографической защиты информации.

12.3. Лица, уполномоченные на обработку персональных данных, имеют право:

- предоставлять персональные данные третьим лицам при наличии согласия на это субъекта персональных данных, а также в других случаях, предусмотренных действующим законодательством;
- мотивированно отказать субъекту персональных данных (его представителю) в удовлетворении запроса о предоставлении информации, касающейся обработки персональных данных субъекта, при наличии оснований, предусмотренных законодательством Российской Федерации.

13. Меры, принимаемые для защиты персональных данных

13.1. Оператор 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 персональных данных.

13.2. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

- Назначение ответственного за организацию обработки персональных данных.

- Осуществление внутреннего контроля и аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.

- Ознакомление лиц, 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.

- Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

- Применение 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.

- Ведение учета машинных носителей персональных данных.

- Выявление фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

- Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- Установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.

- Контроль принимаемых мер по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

- Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

14. Контроль и надзор обработки персональных данных

14.1. Обязанности должностных лиц, осуществляющих контроль обработки и защиту персональных данных, а также их ответственность, определяются в Инструкции ответственного за организацию обработки персональных данных, в Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

14.2. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных назначаются приказом руководителя Оператора из числа лиц, допущенных к обработке персональных данных.

14.3. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора соответствия обработки персональных данных требованиям Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

14.4. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

14.5. Управление Роскомнадзора по Калининградской области:

Адрес: 236022, г. Калининград, ул. Коммунальная, дом 4

Телефон для справок: (4012) 99-40-23

Факс: (4012) 99-40-24

E-mail: rsockanc39@rkkn.gov.ru

Сайт: <http://39.rkn.gov.ru>

Согласно Приказу Роскомнадзора от 28.10.2022 № 179 с 1 марта 2023 года этот срок увеличен. Теперь, если персональных данных изменились, оператору можно отправить соответствующее уведомление в Роскомнадзор не позднее 15-го числа месяца, следующего за месяцем, в котором произошли изменения.

14.6. Лица, уполномоченные на обработку персональных данных, виновные в нарушении требований законодательства в области защиты персональных данных, в том числе допустившие разглашение персональных данных, несут персональную гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

15. Информация об Операторе

15.1.Наименование Оператора: государственное бюджетное учреждение здравоохранения Калининградской области "Балтийская центральная районная больница".

15.2.Юридический адрес (адрес местонахождения): Калининградская область, г. Балтийск, ул. Чехова, д. 11.

16. Заключительные положения

16.1.Настоящая Политика утверждена приказом руководителя Оператора.

16.2.Настоящая Политика обязательна для ознакомления и соблюдения всеми лицами, осуществляющими обработку персональных данных.

16.3.Срок действия Политики – не ограничен.

16.4.Во исполнение части 2 статьи 18.1. Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» настоящая Политика опубликована на сайте Оператора.

16.5.Оператор имеет право вносить изменения в настоящую Политику. Новая редакция Политики вступает в силу с момента ее утверждения руководителем Оператора, если иное не предусмотрено новой редакцией Политики.

16.6.Иные локальные нормативные акты Оператора, регламентирующие порядок защиты и обработки персональных данных, должны издаваться в соответствии с настоящей Политикой и законодательством в области защиты и обработки персональных данных.

16.7.Контроль соблюдения Политики осуществляется руководителем Оператора.