

УТВЕРЖДЕНО

Приказом Главного врача

ГАУЗ ГБ г.Орска от

07.07.2023г. № 362

Политика в отношении обработки персональных данных

ГАУЗ ГБ г.Орска

Настоящая Политика в отношении обработки персональных данных (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о ПДн) и определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных, предпринимаемые ГАУЗ ГБ г.Орска (далее – Оператор).

Целью настоящей 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.

Настоящая Политика применяется ко всем процессам обработки персональных данных, осуществляемых Оператором с использованием средств автоматизации и без использования таких средств.

Настоящая Политика является общедоступным документом и размещается на официальном сайте Оператора в сети Интернет по адресу: <https://orskgb.ru>.

Содержание

1. Общие положения
2. Цели обработки персональных данных и правовые основания обработки персональных данных
3. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных
4. Порядок и условия обработки персональных данных, включая трансграничную передачу
5. Права субъектов персональных данных и порядок их реализации
6. Меры, направленные на защиту персональных данных
7. Заключительные положения

1. Общие положения

1.1. Настоящий документ определяет политику ГАУЗ ГБ г.Орска (далее – Оператор) в отношении обработки персональных данных и направлен на обеспечение реализации принципов законности, конфиденциальности и безопасности информации.

1.2. Политика разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о ПДн) и иными нормативными правовыми актами Российской Федерации в области обработки и защиты персональных данных.

1.3. Политика применяется ко всем процессам обработки персональных данных, осуществляемых Оператором с использованием средств автоматизации и без использования таких средств.

1.4. Основные понятия (определения), используемые в Политике:

- персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (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 (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

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

- распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

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

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

- 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;

- обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;

- оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, состав персональных данных, подлежащих обработке, действия (операции) совершаемые с персональными данными;

- субъект персональных данных – физическое лицо, к которому относятся персональные данные;

- третье лицо – лицо, не являющееся субъектом персональных данных, оператором или обработчиком, а также не являющееся лицом, получившим по поручению оператора полномочия на обработку персональных данных;

- обработчик – лицо, осуществляющее обработку персональных данных по поручению оператора;

- конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным

данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.5. Оператор имеет право поручать обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о ПДн.

1.6. Оператор осуществляет трансграничную передачу персональных данных.

2. Действия с персональными данными, цели обработки персональных данных и правовые основания обработки персональных данных

2.1. Оператор обрабатывает персональные данные для выполнения своей основной деятельности, связанной с оказанием медицинской помощи населению города Орска. Оператор также осуществляет обработку персональных данных своих работников, а также соискателей при трудоустройстве.

2.2. Оператор осуществляет действия с персональными данными - это обработка персональных данных, которая включает в себя различные операции, совершаемые с использованием средств автоматизации или без них. К таким операциям относятся:

- сбор - получение персональных данных из различных источников, в том числе от самих субъектов персональных данных;
- запись - фиксация персональных данных на материальном носителе или в электронной форме;

- систематизация - распределение персональных данных по определенным критериям или группам;
- накопление - создание и увеличение объема базы персональных данных;
- хранение - обеспечение сохранности и целостности персональных данных в течение определенного срока;
- уточнение - обновление или изменение персональных данных в соответствии с действительностью;
- извлечение - получение доступа к персональным данным для их использования, передачи или иных целей;
- использование - действия с персональными данными, направленные на выполнение определенной задачи или функции;
- передача - предоставление доступа к персональным данным определенному лицу или организации;
- распространение - действия, направленные на передачу персональных данных неопределенному кругу лиц или на ознакомление с ними широкой публики;
- обезличивание - действия, в результате которых становится невозможно определить принадлежность персональных данных конкретному субъекту;
- блокирование - временное прекращение обработки персональных данных по какой-либо причине;
- удаление - уничтожение записей о персональных данных в информационной системе или на материальном носителе;
- уничтожение - действия, в результате которых становится невозможно восстановить содержание или форму персональных данных.

Оператор персональных данных может выполнять все эти действия с ПДн своих работников, пациентов и других лиц в соответствии с законодательством и локальными актами. Оператор должен обеспечить защиту ПД от несанкционированного доступа, изменения, уничтожения и других неправомерных действий.

В ГАУЗ ГБ г.Орска осуществляется обработка персональных данных следующих категорий субъектов:

- пациенты
- родственники пациентов и их законные представители;
- работники ГАУЗ ГБ г.Орска
- кандидаты на вакантные должности;
- лица, с которыми заключены договоры гражданско-правового характера;
- представители контрагентов (физические лица);
- посетители ГАУЗ «ГБ г.Орска и сайта ГАУЗ ГБ г.Орска;
- студенты общеобразовательных организаций, проходящие практику в ГАУЗ ГБ г.Орска
- других субъектов персональных данных в соответствие с законодательством РФ

2.3. Цели обработки персональных данных Оператором в зависимости от категорий субъектов персональных данных:

- Персональные данные пациентов обрабатываются для целей:
- оказания медицинской помощи в соответствии с законодательством РФ;
- идентификация пациента и его представителя;

- установление медицинского диагноза;
- выдача медицинских документов пациенту или его представителю;
- защита жизни, здоровья или иных жизненно важных интересов пациентов или других лиц;
- передача медицинской информации о пациенте другим медицинским организациям или специалистам по согласию пациента или в случаях, предусмотренных законом;
- осуществление правосудия;
- статистическая обработка;
- информационное обслуживание пациентов;
- обеспечение безопасности и контроля качества медицинских услуг.
- заключения и исполнения договоров на оказание медицинских услуг;
- проведения медицинских исследований и экспертиз;
- осуществления страхования медицинского риска;
- информирования пациентов о новых медицинских услугах и акциях;
- выполнение требований законодательства.
- Персональные данные сотрудников обрабатываются для целей:
 - заключения и исполнения трудовых договоров;
 - учета и выплаты заработной платы и других вознаграждений;
 - налогообложения и уплаты страховых взносов;
 - организации трудового процесса и внутреннего контроля;
 - обеспечения безопасности персонала и имущества Оператора;
 - соблюдения трудового законодательства и нормативных актов Оператора.

- Персональные данные кандидатов на вакансии обрабатываются для целей:

- подбора и оценки персонала для трудоустройства;
- проверки квалификации и профессиональных навыков;
- информирования о результатах отбора и приглашения на работу.

- Персональные данные поставщиков, контрагентов и иных лиц, с которыми Оператор взаимодействует в рамках своей деятельности, обрабатываются для целей:

- заключения и исполнения гражданско-правовых договоров;
- осуществления расчетов и взаиморасчетов;
- соблюдения законодательства РФ в сфере бухгалтерского учета, налогообложения, аудита и противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

2.4. Правовые основания обработки персональных данных Оператором:

- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федеральный закон от 29.12.2006 № 255-ФЗ «О порядке оказания платных медицинских услуг»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;
- Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ;

- Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ;

- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;

- Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

- договоры на оказание медицинских услуг;

- трудовые договоры с сотрудниками;

- гражданско-правовые договоры с поставщиками, контрагентами и иными лицами;

- согласие на обработку персональных данных.

3. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных.

3.1. Оператор обрабатывает персональные данные в объеме, необходимом для достижения целей обработки, указанных в п. 2.2 настоящей Политики.

3.2. Оператор обрабатывает следующие категории персональных данных:

Персональные данные пациентов, включая:

- фамилию, имя, отчество;

- дату и место рождения;

- пол;

- гражданство;

- адрес регистрации и фактического проживания;

- номер телефона и адрес электронной почты;
- паспортные данные;
- данные полиса обязательного медицинского страхования;
- сведения о состоянии здоровья, медицинской истории, диагнозах, назначениях, результатах анализов и обследований;
- сведения о наличии инвалидности и степени ограничения жизнедеятельности;
- сведения о наличии аллергических реакций или противопоказаний к лекарственным средствам;
- сведения о наличии хронических заболеваний или наследственной предрасположенности к ним;
- сведения о наличии вредных привычек или факторов риска для здоровья;
- сведения о социальном статусе и материальном положении;
- сведения о родственниках или законных представителях.

Персональные данные сотрудников, включая:

- фамилию, имя, отчество;
- дату и место рождения;
- пол;
- гражданство;
- адрес регистрации и фактического проживания;
- номер телефона и адрес электронной почты;
- паспортные данные;
- ИНН и СНИЛС;

- данные трудовой книжки и диплома об образовании;
- данные банковской карты для выплаты заработной платы;
- сведения о составе семьи и наличии иждивенцев;
- сведения о профессиональной квалификации и опыте работы;
- сведения о наличии допуска к работе с персональными данными или другими конфиденциальными сведениями;
- сведения о наличии дисциплинарных взысканий или поощрений, наградах и званиях;
- сведения о повышении квалификации и переподготовки; о результатах аттестации и оценки;
- сведения об ученой степени, об опыте работы, местах предыдущей работы и осуществления предпринимательской деятельности;
- сведения о состоянии здоровья, включая сведения об инвалидности;
- сведения о воинском учете, анкетных и биографических данных;
- сведения о социальных льготах, гарантиях, пенсионном обеспечении и страховании;
- реквизиты банковского счета, необходимые для перечисления заработной платы

Персональные данные кандидатов на вакансии, включая:

- фамилию, имя, отчество;
- дату и место рождения;
- пол;
- гражданство;
- адрес регистрации и фактического проживания;

- номер телефона и адрес электронной почты;
- паспортные данные (при необходимости);
- ИНН и СНИЛС (при необходимости);
- данные трудовой книжки и диплома об образовании;
- сведения о профессиональной квалификации и опыте работы;
- сведения о наличии допуска к работе с персональными данными или другими конфиденциальными сведениями (при необходимости);
- сведения о наличии рекомендаций от предыдущих работодателей.
- Персональные данные поставщиков, контрагентов и иных лиц, с которыми Оператор взаимодействует в рамках своей деятельности, включая:
 - фамилию, имя, отчество;
 - дату и место рождения (при необходимости);
 - пол (при необходимости);
 - гражданство (при необходимости);
 - адрес регистрации и фактического проживания (при необходимости);
 - номер телефона и адрес электронной почты;
 - паспортные данные (при необходимости);
 - ИНН и СНИЛС (при необходимости);
 - данные банковского счета для осуществления расчетов;
 - сведения о предыдущей (щих) должности (тях) и месте (ах) работы.

3.3. Оператор обрабатывает специальные категории персональных данных, относящихся к состоянию здоровья пациентов, на основании ст. 10 Закона о ПДн, а также биометрические персональные данные, относящиеся к физиологическим или биологическим характеристикам пациентов, на

основании ст. 11 Закона о ПДн. Обработка таких данных осуществляется только при наличии письменного согласия пациентов или их законных представителей.

4. Порядок и условия обработки персональных данных, включая трансграничную передачу (при необходимости).

4.1. Оператор обрабатывает персональные данные с соблюдением следующих принципов:

- законности и справедливости основ;
- ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопустимости обработки персональных данных, несовместимой с целями сбора персональных данных;
- недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- недопустимости обработки персональных данных, избыточных 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.

4.2. Оператор осуществляет обработку персональных данных с использованием средств автоматизации и без использования таких средств.

4.3. Оператор осуществляет обработку персональных данных на основании:

- согласия субъекта персональных данных на обработку его персональных данных;

- законодательства РФ или договора, сторонами которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных.

4.4. Оператор получает согласие субъекта персональных данных на обработку его персональных данных в письменной форме при личном подписании документа, содержащего такое согласие, или в электронной форме при подтверждении факта получения электронного сообщения, содержащего такое согласие.

4.5. Согласие на обработку персональных данных должно содержать следующую информацию:

- фамилию, имя, отчество (при наличии) и адрес субъекта персональных данных или представителя субъекта персональных данных;

- наименование или фамилию, имя, отчество (при наличии) и адрес Оператора или представителя Оператора;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие;

- наименование или фамилию, имя, отчество (при наличии) и адрес лица (лиц), осуществляющего(-их) обработку персональных данных по поручению Оператора (если такое поручение предусмотрено);

- способы (методы) обработки персональных данных (если это необходимо для субъекта персональных данных);

- срок, в течение которого действует согласие, а также способ его отзыва, если иное не установлено законодательством РФ;

- подпись субъекта персональных данных или его представителя.

4.6. Оператор обязан прекратить обработку персональных данных в случаях:

- достижения целей обработки персональных данных;

- истечения срока действия согласия субъекта персональных данных или отзыва такого согласия;

- выявления неправомерной обработки персональных данных;

- ликвидации Оператора.

4.7. Оператор осуществляет трансграничную передачу персональных данных на территорию иностранного государства.

Оператор определяет цель и правовое основание трансграничной передачи персональных данных в соответствии с Законом и международными договорами Российской Федерации.

Оператор проверяет, входит ли иностранное государство, на территорию которого планируется передача персональных данных, в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, утвержденный Роскомнадзором. Если нет, то оператор должен получить согласие субъекта персональных данных на такую передачу или доказать наличие иной основы для передачи персональных данных в соответствии со статьей 12 ФЗ-152.

Оператор получает от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым

планируется трансграничная передача персональных данных, сведения о принимаемых ими мерах по защите передаваемых персональных данных и об условиях прекращения их обработки, а также информацию о правовом регулировании в области персональных данных иностранного государства.

Оператор направляет уведомление о намерении осуществлять трансграничную передачу персональных данных в Роскомнадзор в виде документа на бумажном носителе или в форме электронного документа с указанием следующих сведений:

- наименование (фамилия, имя, отчество), адрес оператора, а также дата и номер уведомления о намерении осуществлять обработку персональных данных, ранее направленного оператором в соответствии со статьей 22 Закона;
- наименование (фамилия, имя, отчество) лица, ответственного за организацию обработки персональных данных, номера контактных телефонов, почтовые адреса и адреса электронной почты;
- правовое основание и цель трансграничной передачи персональных данных и дальнейшей обработки переданных персональных данных;
- категории и перечень передаваемых персональных данных;
- категории субъектов персональных данных, персональные данные которых передаются;
- перечень иностранных государств, на территорию которых планируется трансграничная передача персональных данных;
- дата проведения оператором оценки соблюдения органами власти иностранных государств, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача персональных данных, конфиденциальности персональных данных и обеспечения безопасности персональных данных при их обработке.

Оператор осуществляет трансграничную передачу персональных данных после получения подтверждения от Роскомнадзора о регистрации уведомления о намерении осуществлять трансграничную передачу персональных данных, если такое подтверждение требуется в соответствии с Законом.

Оператор обеспечивает защиту передаваемых персональных данных от несанкционированного доступа, изменения, уничтожения, блокирования, копирования, распространения и иных неправомерных действий в соответствии с требованиями Закона и Постановления Правительства РФ от 01.11.2012 № 1119.

Оператор ведет учет трансграничной передачи персональных данных и предоставляет Роскомнадзору информацию о такой передаче по его запросу.

5. Права субъектов персональных данных и порядок их реализации.

5.1. Субъект персональных данных имеет право:

- получать от Оператора информацию, касающуюся обработки его персональных данных, в том числе содержащую:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных Законом о ПДн;

- информацию о проведенной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

- требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- отзывать свое согласие на обработку персональных данных;

- требовать от Оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных.

5.2. Для реализации своих прав субъект персональных данных может обратиться к Оператору лично или направить письменное обращение по почте или электронной почте.

5.3. Обращение субъекта персональных данных должно содержать следующую информацию:

- фамилию, имя, отчество (при наличии) и адрес субъекта персональных данных или его представителя;

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;

- подпись субъекта персональных данных или его представителя.

5.4. Оператор обязан рассмотреть обращение субъекта персональных данных и дать ему письменный ответ в течение 30 дней с даты получения обращения, если иной срок не установлен федеральным законом.

6. Меры, направленные на защиту персональных данных.

6.1. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.2. К таким мерам относятся:

- назначение ответственного за организацию обработки и защиты персональных данных;

- разработка и утверждение локальных актов по вопросам обработки и защиты персональных данных;
- ограничение состава и объема обрабатываемых персональных данных;
- определение угроз безопасности персональных данных при их обработке и разработка мер по защите информации;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе Оператора, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- использование антивирусных программ и средств восстановления системы защиты информации;
- применение процедур контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет материальных носителей персональных данных;
- проведение обучения работников Оператора, осуществляющих обработку персональных данных, основам защиты информации и правилам работы с персональными данными;
- обнаружение фактов несанкционированного доступа к персональным данным и принятием соответствующих мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

- восстановление персональных данных, модифицированных или уничтоженных в следствие несанкционированного доступа к ним;

6.3. Оператор несет ответственность за несоблюдение требований законодательства РФ в области обработки и защиты персональных данных в соответствии с действующим законодательством РФ.

7. Заключительные положения.

7.1. Настоящая Политика вступает в силу с момента ее утверждения руководителем Оператора и действует бессрочно до замены ее новой Политикой.

7.2. Настоящая Политика является локальным нормативным актом Оператора и подлежит обязательному исполнению всеми работниками Оператора, осуществляющими обработку персональных данных.

7.3. Контроль за соблюдением требований настоящей Политики осуществляет ответственный за организацию обработки и защиты персональных данных.

7.4. Все предложения и замечания по улучшению настоящей Политики направляются ответственному за организацию обработки и защиты персональных данных.

7.5. В случае внесения изменений в законодательство РФ в области обработки и защиты персональных данных Оператор вносит соответствующие изменения в настоящую Политику. При этом срок внесения изменений не должен превышать 10 рабочих дней с момента вступления в силу соответствующих изменений законодательства РФ.