



УТВЕРЖДАЮ

Директор ООО «ТРЦ»

С.Р. Аверина

«30» ноября 2016 г.

ПОЛИТИКА

Общества с ограниченной ответственностью «Тюменский реабилитационный центр» В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о ПДн) и является основополагающим внутренним регулятивным документом общества с ограниченной ответственностью «Тюменский реабилитационный центр» (далее - Общество), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Общество.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Обществе, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Обществом как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

2. Информация об операторе и основные понятия

2.1. Полное наименование: Общество с ограниченной ответственностью «Тюменский реабилитационный центр».

2.2. Сокращенное наименование: ООО «ТРЦ».

2.3. Юридический адрес: 625026, г. Тюмень, ул. Республики, д.148, корп. ½.

Адрес обособленного подразделения: 625007 г. Тюмень, ул. Широтная, 29 корп. 3/3.

2.4. Телефон/факс (3452) 34-95-34, 34-97-79, эл.почта: trc72@mail.ru .

2.5. В целях настоящей Политики используются следующие основные понятия:

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

2) **оператор** - 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;

3) **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;

- 4) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
- 5) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 6) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 7) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 8) **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;
- 9) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 10) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- 11) **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Основания обработки и категории персональных данных, обрабатываемых в Обществе

3.1. Обработка ПДн в Обществе осуществляется в соответствии со следующими нормативными правовыми актами Российской Федерации:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 24.11.1995 N 181-ФЗ "О социальной защите инвалидов в Российской Федерации";
- Федеральным законом от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации".

Кроме того, обработка ПДн в Обществе осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Общество выступает в качестве работодателя (гл. 14 Трудового кодекса Российской Федерации), в связи с реализацией Обществом своих прав и обязанностей как юридического лица.

3.2. В рамках оказания комплексной протезно-ортопедической помощи Обществом обрабатываются ПДн физических лиц, получивших направление в Общество для оказания протезно-ортопедической помощи, а также физических лиц обратившихся в Общество для оказания протезно-ортопедической помощи без соответствующего направления.

При этом также обрабатываются ПДн:

- а) застрахованных лиц, пострадавших вследствие несчастного случая на производстве, указанных в реестрах, полученных Обществом от государственных заказчиков, в рамках выполнения заключенных контрактов;
- б) инвалидов и льготных категорий граждан из числа ветеранов, указанных в реестрах, полученных Обществом от государственных заказчиков, в рамках выполнения заключенных контрактов.

3.3. В рамках оказания медицинской помощи Обществом обрабатываются ПДн физических лиц, обратившихся в Общество за получением медицинской помощи.

3.4. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Общество выступает в качестве работодателя, обрабатываются ПДн лиц, претендующих на трудоустройство в Общество, работников Общества (далее - Работники) и бывших Работников.

3.5. В связи с реализацией своих прав и обязанностей как юридического лица, Обществом обрабатываются ПДн физических лиц, являющихся контрагентами (возможными контрагентами) Общества по гражданско-правовым договорам, ПДн руководителя, учредителей и ПДн иных физических лиц, а также граждан, письменно обращающихся в Общество по вопросам его деятельности.

3.6. ПДн получают и обрабатываются Обществом на основании федеральных законов и иных нормативных правовых актов Российской Федерации, а в необходимых случаях - при наличии письменного согласия субъекта ПДн. Все ПДн следует получать непосредственно от субъекта ПДн. Субъект самостоятельно принимает решение о предоставлении своих ПДн и дает письменное согласие на их обработку оператором.

3.7. Общество предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

3.8. В Обществе не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Обществе, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Обществом ПДн уничтожаются или обезличиваются.

3.9. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки.

4. Принципы обеспечения безопасности персональных данных

4.1. Основной задачей обеспечения безопасности ПДн при их обработке в Обществе является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

4.2. Для обеспечения безопасности ПДн Общество руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в Обществе осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

4) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

5) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Обществе с учетом выявления новых способов и средств реализации угроз безопасности ПДн;

6) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

7) минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

8) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Общества (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;

9) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Общества (далее - СЗПДн) не дают возможности преодоления имеющихся в Обществе систем защиты возможными нарушителями безопасности ПДн;

10) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Общества предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Общества до заключения договоров.

5. Доступ к обрабатываемым персональным данным

5.1. Доступ к обрабатываемым в Обществе ПДн имеют лица, уполномоченные приказом директора Общества, а также лица, чьи ПДн подлежат обработке.

5.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой функции Общества закрепляются за соответствующими структурными подразделениями Общества.

Доступ к ПДн, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением Общества, могут иметь только Работники этого структурного подразделения. Работники допускаются к ПДн, связанным с деятельностью другого структурного подразделения, только для чтения и подготовки обобщенных материалов в части вопросов, касающихся структурного подразделения этих Работников.

5.3. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних документов Общества.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами Общества, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

5.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Обществом, определяется в соответствии с законодательством РФ.

5.5. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Обществом;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Обществом способы обработки персональных данных;
- наименование учреждения и место его нахождения, сведения о лицах (за исключением работников Общества), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании законодательства РФ;
- 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 законодательством РФ;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка поручена или будет поручена такому лицу.

5.6. Субъект персональных данных имеет право на получение сведений, указанных в настоящем разделе, за исключением случаев, предусмотренных законодательством РФ.

5.7. Субъект персональных данных вправе требовать от лиц, ответственных за обработку персональных данных в Обществе, уточнения его 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, а также принимать предусмотренные законом меры по защите своих прав.

5.8. Сведения, указанные в настоящем разделе, предоставляются лицами, ответственными за обработку персональных данных в Обществе, субъекту персональных данных в доступной форме.

5.9. Сведения, указанные в настоящем разделе, предоставляются субъекту персональных данных или его представителю лицами, ответственными за обработку персональных данных в Обществе, при получении запроса субъекта персональных данных или его представителя в письменной форме, оформленного в соответствии с требованиями части 3 статьи 14 Федерального закона о персональных данных.

6. Реализуемые требования к защите персональных данных

6.1. Общество принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Законом о ПДн и принятыми в соответствии с ним нормативными правовыми актами, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

6.2. Состав указанных в пункте 6.1 Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а внутренние регулятивные документы об обработке и защите ПДн издаются Обществом исходя из требований:

Закона о ПДн;

главы 14 Трудового кодекса Российской Федерации;

постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

приказа ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн";

постановления Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

постановления Правительства Российской Федерации РФ от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";

иных нормативных правовых актов Российской Федерации об обработке и защите ПДн.

6.3. В предусмотренных законодательством случаях обработка ПДн осуществляется Обществом с согласия субъектов ПДн.

Обществом производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

6.4. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше чем этого требуют цели обработки ПДн, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

6.5. Обществом осуществляется ознакомление работников Общества, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними документами по вопросам обработки ПДн.

6.6. При обработке ПДн с использованием средств автоматизации Обществом, в частности, применяются следующие меры:

1) назначается Ответственный за организацию обработки ПДн, определяется его компетенция;

2) утверждаются внутренние документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

3) осуществляется внутренний контроль соответствия обработки ПДн Закону о ПДн и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним документам Общества.

6.7. Обеспечение безопасности ПДн в Обществе при их обработке в информационных системах персональных данных (далее -ИСПДн) достигается в Обществе, в частности, путем:

1) определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

2) определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности Обществом могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки системы защиты персональных данных проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;

3) применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.

В Обществе, в том числе, осуществляются:

оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

учет машинных носителей ПДн, обеспечение их сохранности;

обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

контроль за принимаемыми мерами по обеспечению безопасности ПДн, уровня защищенности ИСПДн.

6.8. Обеспечение защиты ПДн в Обществе при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

1) обособления ПДн от иной информации;

2) недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;

3) использования отдельных материальных носителей для обработки каждой категории ПДн;

4) принятия мер по обеспечению отдельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;

5) соблюдения требований:

к отдельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;

к уточнению ПДн;

к уничтожению или обезличиванию части ПДн;

к использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них ПДн;

к хранению ПДн, в том числе к обеспечению отдельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.